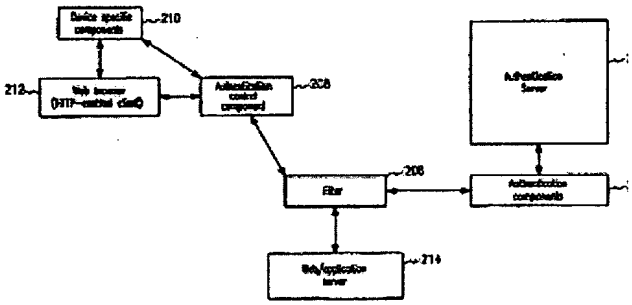
SYSTEM, METHOD AND COMPUTER PROGRAM PRODUCT FOR ENROLLING ANI AUTHENTICATING COMMUNICATION PROTOCOL-ENABLED CLIENTS FOR ACCESS TO INFORMATION

Publication number: JP2003521779T
Publication date: 2003-07-15
Inventor:
Applicant:
Classification:
- international: ***G06F21/20; G06F1/00; G06F21/00; H04L9/32; H04L29/06;*** **G06F21/20; G06F1/00; G06F21/00; H04L9/32; H04L29/06;** (IPC1-7): G06F15/00; H04L9/32
- European: H04L29/06C6C2; G06F21/00N5A; H04L29/06C6B
Application number: JP20010556451T 20010205
Priority number(s): US20000180279P 20000204; US20000185380P 20000228; US20000191471P 20000323; US20000695060 20001025; WO2001US03541 20010205

Also published as:
WO0157669 (A
CA2398584 (A1

Abstract not available for JP2003521779T
Abstract of corresponding document: **WO0157669**

A system, method, and computer program product for allowing access to information, and more particularly to the enrollment and authentication of communication protocol-enabled clients for access to information, particularly confidential information, via the Internet is provided. The system includes client side components (210), a filter (206) coupled to the client side components and server side components (204) coupled to the filter (206). The client side components (210) include an authentication control component (208) that manages the process of capturing user credentials and communicates the result of the capturing process to the filter (206). The authentication server (202) receives the user credentials from the filter (206), attempts to authenticate the user by executing the user policy and communicates to the filter (206) whether the user is authenticated.



(19)日本国特許庁（ＪＰ）　(12)公表特許公報（Ａ）　(11)特許出願公表番号
特表2003－521779
（P2003－521779A）
(43)公表日　平成15年７月15日(2003.7.15)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ｂ	５Ｂ０８５
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７５Ｄ	５Ｊ１０４

審査請求　未請求　予備審査請求　有　（全 55 頁）

(21)出願番号　特願2001－556451(P2001－556451)
(86)(22)出願日　平成13年２月５日(2001.2.5)
(85)翻訳文提出日　平成14年８月５日(2002.8.5)
(86)国際出願番号　ＰＣＴ／ＵＳ０１／０３５４１
(87)国際公開番号　ＷＯ０１／０５７６６９
(87)国際公開日　平成13年８月９日(2001.8.9)
(31)優先権主張番号　６０／１８０，２７９
(32)優先日　平成12年２月４日(2000.2.4)
(33)優先権主張国　米国（ＵＳ）
(31)優先権主張番号　６０／１８５，３８０
(32)優先日　平成12年２月28日(2000.2.28)
(33)優先権主張国　米国（ＵＳ）

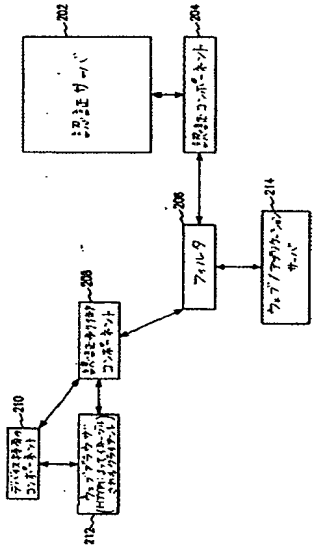
(71)出願人　バイオネトリックス　システムズ　コーポレイション
アメリカ合衆国　バージニア州　22182　ビエンナ，　スイート　500，　ギャロウズ　ロード　1953
(72)発明者　パクシ，　ビクラム　シング
アメリカ合衆国　メリーランド　20832，　オルネイ，　リップリー　マナー　テラス　4648
(74)代理人　弁理士　山本　秀策　（外２名）

Ｆターム(参考)　5B085 AA01 AA08 AE23 BG02 BG03 BG07
5J104 AA09 MA01 PA13

最終頁に続く

(54)【発明の名称】　通信プロトコルによってイネーブルされるクライアントによる情報へのアクセスを登録および認証するためのシステム、方法およびコンピュータプログラム製品

(57)【要約】
情報へのアクセスを可能にするためのシステム、方法、およびコンピュータプログラム製品が提供される。より詳細には、通信プロトコルによってイネーブルされるクライアントがインターネットを介して情報（特に秘匿情報）にアクセスする際の登録および認証を行うためのシステム、方法、およびコンピュータプログラム製品が提供される。上記システムは、クライアント側コンポーネント（２１０）と、上記クライアント側コンポーネントに結合されたフィルタ（２０６）と、上記フィルタ（２０６）に結合されたサーバ側コンポーネント（２０４）とを含む。上記クライアント側コンポーネント（２１０）は、認証制御コンポーネント（２０８）を含む。上記認証制御コンポーネント（２０８）は、ユーザ信用証明書を取得するプロセスを管理し、上記取得プロセスの結果を上記フィルタ（２０６）に通信する。



【特許請求の範囲】

【請求項１】　ユーザがリクエストした情報に通信媒体を介してアクセスする行為を認証するためのシステムであって、

クライアント側コンポーネントと、

該クライアント側コンポーネントに該通信媒体を介して結合されたフィルタと、

該フィルタに該通信媒体を介して結合されたサーバ側コンポーネントと、

を備え、

該クライアント側コンポーネントは、ユーザ信用証明書を取得するプロセスの管理と該ユーザ信用証明書を取得した結果の該フィルタへの通信とを行う認証制御コンポーネントを備え、

該サーバ側コンポーネントは、認証サーバを備え、該認証サーバが、複数のユーザに関連するデータと該ユーザに関連付けられた少なくとも１つの方針とを内部に格納し、該方針は認証レベルを規定し、該認証レベルが、該ユーザが該リクエストされた情報へのアクセス行為について認証を受ける可能性を規定し、該認証サーバは、該ユーザ信用証明書を該フィルタから受信し、該方針を実行することにより該ユーザを認証しようとし、該ユーザが認証されたか否かについて該フィルタに通信し、

該ユーザが該認証サーバによって認証されると、該フィルタは、該リクエストされた情報を含むサーバとインターラクトする、

システム。

【請求項２】　前記通信媒体はインターネットである、請求項１に記載のシステム。

【請求項３】　前記通信媒体はローカルネットワークである、請求項１に記載のシステム。

【請求項４】　前記通信媒体は無線ネットワークである、請求項１に記載のシステム。

【請求項５】　前記サーバはウェブサーバである、請求項１に記載のシステム。

【請求項６】　前記サーバはアプリケーションサーバである、請求項１に記載のシステム。

【請求項７】　前記認証制御コンポーネントは、呼び出されるたびに保全性に関するチェックを受ける、請求項１に記載のシステム。

【請求項８】　リクエストされた情報にアクセスするためにユーザが通信媒体を介してユーザ信用証明書を遠隔的に登録することを可能にするシステムであって、

クライアント側コンポーネントと、

該クライアント側コンポーネントに該通信媒体を介して結合されたフィルタと、

該通信媒体を介して該フィルタに結合されたサーバ側コンポーネントと、

を備え、

該クライアント側コンポーネントは、認証制御コンポーネントおよび登録アプリケーションを備え、該登録アプリケーションは、提示論理を駆動する役割を担い、該提示論理は、ユーザ信用証明書の提示の際に該ユーザと対話し、該認証制御コンポーネントは、ユーザ信用証明書を取得するプロセスの管理と該ユーザ信用証明書を取得した結果の該サーバ側コンポーネントへの通信とを行う役割を担い、

該サーバ側コンポーネントは認証サーバを備え、該認証サーバは、複数のユーザに関連するデータと該ユーザに関連付けられた少なくとも１つの方針とを内部に格納し、該方針は認証レベルを規定し、該認証レベルは、該ユーザが該リクエストされた情報へのアクセス行為について認証を受ける可能性を規定し、該認証サーバは該ユーザ信用証明書を格納する、

システム。

【請求項９】　前記通信媒体はインターネットである、請求項８に記載のシステム。

【請求項１０】　前記通信媒体はローカルネットワークである、請求項８に記載のシステム。

【請求項１１】　前記通信媒体は無線ネットワークである、請求項８に記載

のシステム。

【請求項１２】　リクエストされた情報に通信媒体を介してアクセスする行為についてユーザを認証する方法であって、

複数のユーザに関連するデータと該ユーザに関連付けられた少なくとも１つの方針とを認証サーバに格納する工程であって、該方針は認証レベルを規定し、該認証レベルは、該ユーザが該リクエストされた情報へのアクセス行為について認証を受ける可能性を規定する、工程と、

該ユーザ信用証明書を取得するプロセスを認証制御コンポーネントを介して管理する工程と、

該ユーザ信用証明書を取得した結果を該認証制御コンポーネントから該通信媒体を介してフィルタへと通信させる工程と、

該ユーザ信用証明書を該フィルタから該通信媒体を介して該認証サーバへと通信させる工程と、

該認証サーバが該方針を実行することにより該ユーザを認証すべきか否かを判定する工程と、

該ユーザが認証を受けたか否かを該認証サーバから該通信媒体を介して該フィルタに通信させる工程と、

該ユーザが該認証サーバによって認証された場合、該フィルタと、該リクエストされた情報を含むサーバとをインターラクトさせる工程と、

を包含する、方法。

【請求項１３】　前記通信媒体はインターネットである、請求項１２に記載の方法。

【請求項１４】　前記通信媒体はローカルネットワークである、請求項１２に記載の方法。

【請求項１５】　前記通信媒体は無線ネットワークである、請求項１２に記載の方法。

【請求項１６】　前記サーバはウェブサーバである、請求項１２に記載の方法。

【請求項１７】　前記サーバはアプリケーションサーバである、請求項１２

に記載の方法。

【請求項１８】　前記認証制御コンポーネントは、呼び出されるたびに保全性に関するチェックを受ける、請求項１２に記載の方法。

【請求項１９】　リクエストされた情報にアクセスするためにユーザが通信媒体を介してユーザ信用証明書を遠隔的に登録することを可能にする方法であって、

複数のユーザに関連するデータと該ユーザに関連付けられた少なくとも１つの方針とを認証サーバに格納する工程であって、該方針は認証レベルを規定し、該認証レベルは、該ユーザが該リクエストされた情報へのアクセス行為について認証を受ける可能性を規定する、工程と、

登録アプリケーションによって提示論理を駆動する工程であって、該提示論理は、ユーザ信用証明書の提示の際にユーザと対話する、工程と、

該ユーザ信用証明書を取得するプロセスを認証制御コンポーネントを介して管理する工程と、

該ユーザ信用証明書を取得した結果を該認証制御コンポーネントから該通信媒体を介して認証サーバへと通信させる工程と、

該ユーザ信用証明書を該認証サーバに格納する工程と、

を包含する、方法。

【請求項２０】　前記通信媒体はインターネットである、請求項１９に記載の方法。

【請求項２１】　前記通信媒体はローカルネットワークである、請求項１９に記載の方法。

【請求項２２】　前記通信媒体は無線ネットワークである、請求項１９に記載の方法。

【請求項２３】　ユーザがリクエストした情報に通信媒体を介してアクセスする行為を認証するためのシステムであって、

クライアント側コンポーネントと、

該通信媒体を介して該クライアント側コンポーネントに結合されたサーバ側コンポーネントと、

を備え、
該クライアント側コンポーネントは、ユーザ信用証明書を取得するプロセスの管理と該ユーザ信用証明書を取得した結果の該サーバ側コンポーネントへの通信とを行う認証制御コンポーネントを備え、
該サーバ側コンポーネントは、認証サーバおよびフィルタを備え、該認証サーバは、複数のユーザに関連するデータと該ユーザに関連付けられた少なくとも１つの方針とを内部に格納し、該方針は認証レベルを規定し、該認証レベルは、該ユーザが該リクエストされた情報へのアクセス行為について認証を受ける可能性を規定し、該認証サーバは、該フィルタから該ユーザ信用証明書を受信し、該方針を実行することにより該ユーザを認証し、該ユーザが認証されたか否かについて該フィルタに通信しようとし、該ユーザが該認証サーバによって認証されると、該フィルタは、該リクエストされた情報を含むサーバとインターラクトする、システム。
【請求項２４】　リクエストされた情報に通信媒体を介してアクセスする行為についてユーザを認証する方法であって、
複数のユーザに関連するデータと該ユーザに関連付けられた少なくとも１つの方針とを認証サーバに格納する工程であって、該方針は認証レベルを規定し、該認証レベルは、該ユーザが該リクエストされた情報へのアクセス行為について認証を受ける可能性を規定する、工程と、
該ユーザ信用証明書を取得するプロセスを認証制御コンポーネントを介して管理する工程と、
該ユーザ信用証明書を取得した結果を該認証制御コンポーネントから該通信媒体を介して該認証サーバへと通信させる工程と、
該認証サーバが該方針を実行することにより該ユーザを認証すべきか否かを判定する工程と、
該ユーザが認証を受けたか否かを該認証サーバから該通信媒体を介して該リクエストされた情報を含むサーバに通信させる工程と、
を包含する、方法。

【発明の詳細な説明】

【０００１】

（発明の背景）

（発明の分野）

本発明は概して、情報へのアクセスを可能にするためのシステム、方法およびコンピュータプログラム製品に関し、より詳細には、通信プロトコルによってイネーブルされるクライアントが通信媒体を介して情報（特に秘匿情報）にアクセスする際に上記クライアントの登録および認証を行うためのシステム、方法およびコンピュータプログラム製品に関する。

【０００２】

（関連分野）

現在、経済における情報への迅速なアクセスおよび情報の交換の重要性は、いくら強調してもしたりないくらい重要である。その重要性は、インターネット、イントラネット、情報の無線によるやりとりなどが指数関数的に浸透していることからも分かる。インターネットは相互に接続されたコンピュータネットワークが世界規模になったものであり、インターネットを用いれば、ますます多くの量および種類の情報に電子的にアクセスすることができるようになってきている。今日、インターネットにおける高速アクセスおよび公開情報すなわち非秘匿情報のやり取りは格段の進歩を遂げている。

【０００３】

インターネット上の情報にアクセスするための１つ方法として公知のものに、Ｗｏｒｌｄ　Ｗｉｄｅ　Ｗｅｂ（ｗｗｗ、または「ウェブ」）がある。ウェブは分散型のハイパーメディアシステムであり、クライアントーサーバベースの情報提示システムとして機能する。ウェブは、ハイパーテキストマークアップ言語（ＨＴＭＬ）と呼ばれる言語でフォーマットされた言語をサポートする。ＨＴＭＬ文書は、他の文書ならびにグラフィックファイル、音声ファイルおよび映像ファイルなどへのリンクをサポートする。さらに、ＨＴＭＬは、ウェブページのフォーマット様式および表示様式も制御する。コンピュータユーザは、「クライアント」と呼ばれる汎用コンピュータを用いてウェブ（またはＨＴＭＬ）ページのユ

ニフォームリソースロケーター（ＵＲＬ）を指定することにより、当該ページにアクセスすることができる。図１は、インターネットに接続された複数のクライアントおよびサーバを示すネットワークのブロック図である。

【０００４】

インターネットの浸透が一因となって、どんなユーザもインターネットの機能によって利点を得ることができるようにするためのツールまたはプロトコルがに開発されきている。その例を挙げると、ウェブブラウザ、ＨＴＴＰ、ＳＨＴＴＰ、クッキーおよびＳＳＬがある（ただし、これらに限定されない）。以下、これらの各々についてより詳細に説明する。

【０００５】

ウェブブラウザは、ユーザがウェブページを探して表示する作業を容易にするソフトウェアアプリケーションである。ウェブブラウザの例としては、ネットスケープナビゲータおよびＭｉｃｒｏｓｏｆｔ（登録商標）のインターネットエクスプローラがある。ウェブブラウザは、本明細書中に記載の通信プロトコルによってイネーブルされるクライアントの一例である。通信プロトコルによってイネーブルされるクライアントの他の例を挙げると、ＴＣＰ／ＩＰクライアントおよび無線クライアントがある（ただし、これらに限定されない）。

【０００６】

ハイパーテキスト転送プロトコル（ＨＴＴＰ）は、ウェブによって用いられる共通プロトコルである。ＨＴＴＰは、メッセージのフォーマット方式および送信方式と、ウェブサーバおよびブラウザが様々なコマンドに応答したときにとるべきアクションとを規定する。例えば、ユーザが自身のブラウザ内のＵＲＬに入ると、リクエストされたウェブページをフェッチして送信することをウェブサーバに命令する旨のＨＴＴＰコマンドが実際にウェブサーバに送られる。

【０００７】

ＨＴＴＰが支配関係を持たない（ｓｔａｔｅｌｅｓｓ）プロトコルであると言われている所以は、各コマンドの実行が個別に行われ、当該コマンドの前または後に来るコマンドに関する知識は用いられないことから来ている。これは、ユーザ入力に知的に反応するウェブサイトをインプリメントすることが困難である１

つの原因となっている。このようなＨＴＴＰの特徴に対する対策として取り組まれている技術として、ＨＴＴＰを補足する（ｃｏｍｐｌｉｍｅｎｔ）ための複数の新技術（例えば、ＡｃｔｉｖｅＸ、Ｊａｖａ（Ｒ）、Ｊａｖａ（Ｒ）Ｓｃｒｉｐｔおよびクッキー）がある。

【０００８】

例えば、クッキーは、ウェブサーバがウェブブラウザに与えるメッセージである。クッキーは、サーバ側の接続部がクライアント側の接続部にある情報の格納および検索のどちらを行う際にも用いることができる包括的メカニズムである。このようにしてクライアント側の状態がシンプルかつ永続的な様式で分かると、ウェブーベースのクライアント／サーバアプリケーションの能力が大幅に伸びる。

【０００９】

ＨＴＴＰオブジェクトをユーザに返送する際、サーバも、ユーザによって格納される状態情報を送ることができる。このような状態オブジェクト中には、当該状態が有効となるＵＲＬの範囲の記述が含まれる。将来ユーザが作成した任意のＨＴＴＰリクエストでこの範囲内に収まるものは、状態オブジェクトの現在値をユーザからサーバに返送する伝達を含む。このような状態オブジェクトがクッキーである。この簡単なメカニズムにより、新種のアプリケーションのホストをウェブーベースの環境に合わせて書くことを可能にする強力なツールが得られる。これにより可能になっていることを挙げると、ショッピングアプリケーションにおいて、現在ユーザが選択しているアイテムに関する情報を保存することが可能となり、料金を要求する（ｆｏｒ－ｆｅｅ）サービスにおいて、登録情報を返送することにより、ユーザが次回接続した際に再度ユーザ名（またはユーザＩＤ）をタイプ入力しなくてもよくなり、サイトは、ユーザ選好情報をユーザ単位でユーザコンピュータ上に格納し、ユーザがサイトに接続するたびにこのような選好情報を供給させることができるようになっている。

【００１０】

ウェブ上で用いられる別の共通プロトコルとして、Ｓｅｃｕｒｅ　Ｓｏｃｋｅｔ　Ｌａｙｅｒ（ＳＳＬ）プロトコルがある。ＳＳＬは、プライベート文書をイ

ンターネット経由で送信する際に用いられるプロトコルである。ＳＳＬは、特定のセッションに関わるウェブブラウザのみが知っているプライベートセッションキーを用いることにより、機能する。このセッションキーは、各セッションごとに変更される。このセッションキーを用いて、ＳＳＬ接続を介して転送されたデータを暗号化する。多くのウェブサイトが、秘匿ユーザ情報（例えば、クレジットカード番号）を入手する際にＳＳＬプロトコルを用いている。

【００１１】

ウェブ経由のデータ送信をセキュアに行うための別のプロトコルとして、Ｓｅｃｕｒｅ　ＨＴＴＰ（Ｓ－ＨＴＴＰ）がある。ＳＳＬではクライアントとサーバとの間のセキュアな接続を任意の量のデータをセキュアに送信できるように生成しているのに対し、Ｓ－ＨＴＴＰは、個々のメッセージをセキュアに送信するように設計されている。従って、ＳＳＬおよびＳ－ＨＴＴＰは、競合テクノロジーというよりも相補関係にあテクノロジーとしてみることができる。

【００１２】

上述したように、現在、経済における情報への迅速なアクセスおよび情報の交換の重要性は、いくら強調してもしたりないくらい重要である。上述したようなウェブブラウザおよび様々なプロトコルの登場により、インターネットはますます浸透の度合いを高めている（イントラネットおよび無線通信も、専用のプロトコルを通じてますます浸透の度合いを高めている）。インターネット経由での非秘匿情報のやり取りが高速化したことも、ユーザにとって有用となっている。しかし、そこには問題がある。１つの問題としては、インターネットを通過する秘匿情報の保護がある。別の問題としては、個々のユーザの秘匿情報がインターネットを通過する際にその秘匿状態が保たれているという安心感を満足させることがある。

【００１３】

インターネット経由でユーザに提供されるアプリケーションまたはサービスにおいて秘匿ユーザ情報のアクセスまたは交換が必要になる度合いが高まるにつれ、ユーザの安心感を満たすことの重要性も高まる。このようなアプリケーションまたはサービスの例を挙げると、企業間の電子商取引および企業／消費者間の電

子商取引、オンラインアプリケーション（例えば、バンキング、株式取引、ショッピング、個人化されたコンテンツのウェブサイトなどがある。不適切なユーザに秘匿情報が与えられるのを防ぐために、ユーザ（または通信プロトコルによってイネーブルされるクライアント（例えば、ウェブブラウザ）が）ウェブアプリケーションにアクセスする前に、当該ユーザ（またはクライアント）を認証することが必要である。情報のアクセスおよびやり取りが簡単であることはどのユーザにとっても魅力である一方、ほとんどのユーザは、自身の秘匿情報がインターネット、イントラネット、無線ネットワークなどを介してアクセス可能であるときのセキュリティについても懸念している。そのため、インターネットを用いた情報のアクセスおよびやり取りの浸透速度を妨げないようにするために、インターネットによって情報を提供する者は、秘匿情報の適切な保護と、インターネット経由での情報のアクセスおよびやり取りとの間のバランスをとらなくてはならない。

【００１４】

（発明の要旨）

情報にアクセスすることを可能にするシステム、方法、およびコンピュータプログラム製品が提供され、より詳細には、通信媒体を介して情報（特に、秘密情報）にアクセスするために、通信プロトコルによってイネーブルされるクライアントの登録および認証が提供される。

【００１５】

通信媒体を介してリクエストされた情報にアクセスするために、ユーザを遠隔的に登録および認証するシステムは、クライアント側コンポーネント、通信媒体を介してクライアント側コンポーネントに結合されたフィルタ、および、通信媒体を介してフィルタに結合されたサーバ側コンポーネントを含む。クライアント側コンポーネントは、ユーザ信用証明書（ｃｒｅｄｅｎｔｉａｌ）を取り込み、取り込みプロセスの結果をフィルタに伝えるプロセスを管理する認証制御コンポーネントを含む。サーバ側コンポーネントは、認証サーバを含む。認証サーバは、複数のユーザに関連するデータ、および、ユーザに関連する少なくとも１つの方針（ｐｏｌｉｃｙ）を格納する。ユーザ方針は、認証レベルを決定し、認証レ

ベルは、リクエストされた情報にユーザがアクセスすることを許可される可能性を決定する。さらに、認証サーバは、フィルタからユーザ信用証明書を受信し、ユーザ方針を実行することによりユーザを認証することを試み、ユーザが認証されたかどうかをフィルタに伝える。最終的に、フィルタは、ユーザが認証サーバによって一旦認証されると、リクエストされた情報を含むサーバとインターラクトする。

【００１６】

ユーザの遠隔登録を可能にするため、本発明は、認証制御コンポーネントおよび登録アプリケーションを含むクライアント側コンポーネントを提供する。登録アプリケーションは、ユーザ信用証明書を提示する際にユーザと対話する提示論理を駆動する責任がある。認証制御コンポーネントは、ユーザ信用証明書を取り込み、取り込みプロセスの結果をサーバ側コンポーネントに伝えるプロセスを管理する責任がある。

【００１７】

本発明は、添付の図面を参照して説明される。

【００１８】

（好適な実施形態の詳細な説明）

（Ａ．発明の概要）

本発明の発明者は、秘密情報の保護と、通信媒体（例えば、インターネット）を介して同じ秘密情報にアクセスする容易さとを有効にバランスをとる解決策が存在しなかったことを認識した。本発明は、インターネットを参照して説明されるが、これは、本発明を制限することを意図しないことに留意することが重要である。本発明は、さらに、イントラネット、無線ネットワークなどに適用する。

【００１９】

上記の問題に対する本発明の一般的な解決策は、２通りに分けられる。第１に、出来る限り適切な識別デバイスを使用して、インターネット上で入手可能な秘密情報を保護すること。第２に、適切な識別デバイスを利用して、秘密情報を管理するインターネットによってアクセス可能なアプリケーションおよび／またはサービスに対してユーザを有効に認証するシステム、方法、およびコンピュータ

プログラム製品を提供すること。この認証のためのシステム、方法、およびコンピュータプログラム製品は、インターネットによって現在提供されている情報への素早いアクセスおよび情報の素早い交換という点でのインターネットの評判を下げるべきではない。より詳細には、本発明のシステムのアーキテクチャは、通信プロトコルによってイネーブルされるクライアントを認証するため、かつ、通信プロトコルによってイネーブルされるクライアントの信用証明書を遠隔登録するために、クロスプラットフォーム、高性能、拡張可能、および、高度に拡大縮小可能な解決策である必要がある。

【００２０】

秘密情報の不適切な認証、従って、不適切な保護のために、何千もの電子商取引ビジネス、インターネットデータコンテンツプロバイダなどによって何十億ドルもの損害が出ている。多くのユーザは、インターネットを介して彼らの秘密情報がアクセス可能であることに不愉快さを感じている。従って、秘密情報に関して、これらのユーザは、インターネットの使い易さを諦め、インターネットによってアクセス可能でない、より伝統的なタイプのビジネスまたはサービスに頼るかもしれない。

【００２１】

今日、ほとんどのウェブアプリケーション／サービスは、ユーザ名およびパスワードのみによってユーザを認証する。他の識別デバイスは、スマートカード、トークン、および種々のバイオメトリックデバイスを含むが、これらに制限されない。さらに、ほとんどのウェブアプリケーションは、パスワードのみを伴う「シングルサインオン」と呼ばれるプロセスを取り入れることにより、その秘密データ保護を管理する費用および複雑さを減少させる。シングルサインオンは、各ユーザに、全てのウェブアプリケーションリソース（公開情報または秘密でない情報および秘密情報を含む）にアクセスするための１つのパスワードを提供する。ほとんどのユーザは、書き留めることなく１つのパスワードを記憶することが出来る。これにより、情報保護を管理する複雑さおよび費用が減少されるが、情報にアクセスするユーザが認証されたユーザである可能性が減少される。パスワードを使用するシングルサインオンは、秘密でない情報にアクセスするユーザを

認証することが可能であるが、パスワードを使用するシングルサインオンは、他のタイプの情報に加え、秘密情報にアクセスするユーザを認証することが可能でない。アクセスするユーザが認証されたユーザである可能性は、複数のパスワード、トークン、スマートカード、またはバイオメトリックデバイスを使用して、異なるタイプの情報（例えば、秘密情報対秘密でない情報）にアクセスすることを各ユーザに強制することにより増加し得る。

【００２２】

（Ｂ．システムアーキテクチャの概要）

図２は、本発明の例示的な動作環境を表すブロック図である。図２の例示的な動作環境は、例示的な目的のためだけに示され、本発明を制限しないことが理解されるべきである。本明細書中に示す動作環境の他の実施形態は、本明細書中に含まれる教示に基づいて、関連分野（単数または複数）の当業者に明らかであり、本明細書は、このような他の実施形態に向けられる。図２を参照すると、認証サーバ２０２、認証コンポーネント２０４、フィルタ２０６、認証制御コンポーネント２０８、デバイス特有のコンポーネント２１０、ウェブブラウザ２１２、およびウェブ／アプリケーションサーバ２１４が示される。

【００２３】

本発明の機能モジュールまたはコンポーネントの実施形態は、認証サーバ２０２、認証コンポーネント２０４、フィルタ２０６、および認証制御コンポーネント２０８を含む。本発明のコンポーネントは、それぞれ、下記のカテゴリの下で分類され得る：クライアント側コンポーネント；フィルタコンポーネント；サーバ側コンポーネントおよび遠隔登録コンポーネント。認証サーバ２０２および認証コンポーネント２０４は、サーバ側コンポーネントとして分類される。認証制御コンポーネント２０８は、デバイス特有のコンポーネント２１０およびウェブブラウザ２１２と共に、クライアント側コンポーネントとして分類される。フィルタ２０６は、フィルタコンポーネントとして分類される。最後に、認証制御コンポーネント２０８および認証コンポーネント２０４は、遠隔登録コンポーネントとして分類される。本発明のある実施形態において、サーバ側コンポーネントおよび遠隔登録コンポーネントは、プラットフォームに依存しないように設計さ

れ、これらとの通信が標準の公開プロトコル（例えば、ＨＴＴＰプロトコル（ＲＦＣ２０６８））を介して行われることだけを必要とする。認証制御コンポーネント２０８が、クライアント側コンポーネントおよび遠隔登録コンポーネントの両方として分類されることに留意されたい。さらに、認証コンポーネント２０４は、サーバ側コンポーネントおよび遠隔登録コンポーネントの両方として分類される。本発明の異なる分類（または、機能）におけるこれらのコンポーネントの再使用は、オブジェクト指向のプログラミング言語においてこれらのコンポーネントを実施した結果である。

【００２４】

任意のオブジェクト指向プログラムの利点は、プログラマーが、新しいオブジェクトが追加される場合に変更される必要がないモジュール（機能を実行するモジュール）を作成することを可能にすることである。オブジェクトは、タスクを実行するために必要なデータおよび機能の両方を含む。従って、本発明のコンポーネントによってオブジェクトとして実行されるべき機能を実施することにより、作成されたモジュールは、新しいタイプのオブジェクト（または、機能）が追加される場合に変更される必要がない。本発明のこの実施によって、複雑さが減少され、従って、効率が増加させられる。本発明のカテゴリ（および、それぞれのコンポーネント）について、下記で説明する。

【００２５】

（１．サーバ側コンポーネント）

上記のように、認証サーバ２０２および認証コンポーネント２０４は、サーバ側コンポーネントとして分類される。認証サーバ２０２は、認証コンポーネント２０４に接続される（図２参照）。認証サーバ２０２は、本発明に関連する同時係属中の米国出願第０９／２６４，７２６号および米国出願第０９／５１７，１２１号で詳細に説明される（上記の「関連出願の相互参照」を参照）。便宜上、認証サーバ２０２について下記で簡単に説明する。

【００２６】

認証サーバ２０２は、本発明のエンジンであり、本発明によって必要とされるデータの集まりを格納する。エンジンの機能および認証サーバ２０２内に格納さ

れるデータの機能の両方について、下記により詳細に説明する。認証サーバ２０２内に格納されるデータのタイプは、部分的には、登録ステーションおよび管理ステーション（図示せず）の動作を介して決定される。登録ステーションを使用して、本発明によって認証されるべきユーザを登録する。登録ステーションには、ユーザを登録するため、かつ、最終的には認証するために、本発明によって使用される全てのタイプのデバイス（例えば、指紋スキャナ、音声または顔面認識システムなどのバイオメトリックデバイス、あるいは、ＲＳＡトークン、ＶＡＳＣＯトークンなどの安全トークンなど）が取り付けられている。ユーザが本発明に登録されると、ユーザは、アドミニストレータが必要だと思うだけの数のデバイスに登録され得る。

【００２７】

本発明のアドミニストレータによって管理ステーションが使用されて、全体的な管理デューティが実行される。アドミニストレータは、さらに、管理ステーションを使用して、種々のレポートを生成し得る。レポートは、認証サーバ２０２内に格納される異なるタイプのデータのリスト（例えば、本発明において現在登録されているユーザのリスト）を含み得る。さらに、典型的には、管理ステーションを使用して、認証サーバ２０２内に初期データがセットアップされる。

【００２８】

本発明によって使用され得る別のコンポーネントは、図２に示さない衛星登録ステーションである。衛星登録ステーションを使用して、遠隔地において、ユーザを本発明に登録する。衛星登録ステーションには、管理ステーションと同じだけの数のデバイスが取り付けられるが、代わりに、管理ステーションの縮小されたバージョンでもあり得る。下記で詳細に説明するように、本発明は、ウェブブラウザ（すなわち、通信プロトコルによってイネーブルされるクライアント）が、遠隔登録ステーションとして機能することを可能にする。

【００２９】

上記のように、認証サーバ２０２は、認証コンポーネント２０４に接続される。認証コンポーネント２０４は、ｌｉｓｔｅｎオブジェクト、ｃｏｍｍオブジェクト、および認証オブジェクト（下記で説明する）を含む特定の機能を実行する

異なるタイプのオブジェクトを含む。これらのタイプのオブジェクトは、ユーザが認証されることを試みる場合に、本発明によって使用される。上記のように、本発明は、秘密情報の保護と、インターネットなどの通信媒体を介して同じ秘密情報にアクセスする容易さとを有効にバランスをとる解決策を提供する。本発明は、インターネットを参照して説明されるが、これは、本発明を制限することを意図しないことに留意することが重要である。本発明は、さらに、イントラネット、無線ネットワークなどに適用する。通信媒体のタイプによって、認証コンポーネント２０４は、その特定の媒体を介してユーザを認証するために必要な機能を実行する。これについて、図４、図５Ａ、および図５Ｂを参照して示す。

【００３０】

図４において、認証コンポーネント２０４は、無線ネットワークに必要な機能を実行する。図５Ａは、ローカルネットワークまたはイントラネットに必要な機能を実行する認証コンポーネント２０４を示す。最後に、図５Ｂは、インターネットに必要な機能を実行する認証コンポーネント２０４を示す。通信媒体がインターネットである場合の認証コンポーネント２０４について下記で説明するが、本発明は、インターネットに制限されない。

【００３１】

（ａ．ｌｉｓｔｅｎオブジェクト）

ｌｉｓｔｅｎオブジェクトは、起動の際に認証サーバ２０２によって具現化される。ｌｉｓｔｅｎオブジェクトは、図６によって示すように、下記のタスクを行う責任がある。図６において、フローチャートがステップ６０２から始まる。一旦具現化されると、ｌｉｓｔｅｎオブジェクトは、ステップ６０２によって示すように、標準ＳＳＬポート（すなわち、ポート４４３）で入来するＳＳＬ接続リクエストをリッスン（ｌｉｓｔｅｎ）するＨＴＴＰデーモンのように機能する。その後、制御はステップ６０４に移動する。

【００３２】

ステップ６０４において、ｌｉｓｔｅｎオブジェクトがＳＳＬ接続リクエストを一旦受信すると、ｌｉｓｔｅｎオブジェクトは、下記で説明するように、ｃｏｍｍオブジェクトおよび／または認証オブジェクトによってリクエストが処理さ

れることを保証する。その後、制御はステップ６０２に戻り、ここで、ｌｉｓｔｅｎオブジェクトは、入来するＳＳＬ接続リクエストをリッスンする。ｌｉｓｔｅｎオブジェクトが破壊されるのは、認証サーバ２０２がオフになってからのみである。

【００３３】

ステップ６０４においてリクエストが処理されることをｌｉｓｔｅｎオブジェクトが保証する異なる方法がある。例えば、本発明のある実施形態において、ｌｉｓｔｅｎオブジェクトは、標準デーモンスレッド、ワーカースレッドプールモデルとして実施され得る。ここで、単一のデーモンスレッドは、入来する全ての接続リクエストを受信し、プール内のワーカースレッドの１つに、新しく生成されたソケット（各接続のためのソケット）を引き渡す。その後、デーモンスレッドは、さらなる入来接続をリッスンするために戻り得る。プール内のスレッドの数は、構成可能なパラメータであり得る。スレッドは、関連分野で周知である。

【００３４】

本発明の別の実施形態において、ｌｉｓｔｅｎオブジェクトは、ＩＯ完了ポートを使用して、クライアントからリクエストを受信し、かつ、クライアントに応答を転送する単一のポイントを提供し得る。この技術は、ＩＯ中心処理の性能を向上することが証明されている非同期通信メカニズムにも必然的に向いている。ＩＯ完了ポートおよび非同期通信メカニズムも、関連分野で周知である。本発明のｃｏｍｍオブジェクトについて、下記で説明する。

【００３５】

（ｂ．ｃｏｍｍオブジェクト）

ｃｏｍｍオブジェクトは、それぞれの新しいクライアントセッションに関して具現化される。クライアントセッションは、ウェブブラウザ２１２におけるユーザが、ウェブ／アプリケーションサーバ２１４にアクセスしようと試みる場合に生じる。認証プロセスが一旦完了すると、エラーまたはタイムアウトが生じて、対応するｃｏｍｍオブジェクトが破壊される。ｃｏｍｍオブジェクトは、図７によって示すような下記のタスクを行う責任がある。図７において、ステップ７０２からフローが始まる。ステップ７０２において、ｃｏｍｍオブジェクトは、デ

ータの対称的な暗号化／復号化に関するセッションキーに関して、ウェブブラウザ２１２と交渉する。これは、サーバ側の証明書（ｃｅｒｔｉｆｉｃａｔｅ）およびクライアント側の証明書の交換を伴い得る。その後、制御はステップ７０４に移動する。

【００３６】

ステップ７０４において、ｃｏｍｍオブジェクトは、セッションキーによって暗号化されたデータをウェブブラウザ２１２から受信する。その後、制御はステップ７０６に移動する。

【００３７】

ステップ７０６において、ｃｏｍｍオブジェクトは、ステップ７０４において受信したデータを復号化する。その後、制御はステップ７０８に移動する。

【００３８】

ステップ７０８において、ｃｏｍｍオブジェクトは、ＨＴＴＰヘッダーおよび復号化データ内のコンテンツを構文解析する。その後、制御はステップ７１０に移動する。

【００３９】

ステップ７１０において、ｃｏｍｍオブジェクトとは、特定のフォーマットと一致するデータオブジェクトを受信したデータから作成し、認証オブジェクトまたは方針オブジェクトに引き渡し、ＨＴＴＰ仕様書によってフォーマットする。方針オブジェクトは、本発明に関連する同時係属中の米国出願第０９／２６４，７２６号および米国出願第０９／５１７，１２１号で詳細に説明される。方針オブジェクトは、使用される特定の方針によって異なる。方針は、認証サーバ２０２によってユーザが認証される方法または手段を決定する。ユーザは、適切な方針をパスするまで認証されないことを留意することが重要である。本発明において、ユーザは、自分の方針をパスせずに、１つ以上のデバイスをただ単にパスするだけでは、決して認証されない。方針について、下記でより詳細に説明する。その後、制御はステップ７１２に移動する。

【００４０】

ステップ７１２において、ｃｏｍｍオブジェクトは、認証オブジェクトまたは

方針オブジェクトからデータオブジェクトを受信し返し、ＨＴＴＰ仕様書によってそれをフォーマットする。その後、制御はステップ７１４に移動する。

【００４１】

ステップ７１４において、ｃｏｍｍオブジェクトは、ウェブブラウザ２１２に送信し返すべきセッションキーによってデータを暗号化する。その後、制御はステップ７１６に移動する。

【００４２】

ステップ７１６において、ｃｏｍｍオブジェクトは、暗号化されたデータをウェブブラウザ２１２に送信する。方針が多元的な認証を必要とする場合、上記のステップのいくつかまたは全てが数回繰り返され得ることを留意することが重要である。図７のフローチャートは、この時点で終了する。上記のように、ｃｏｍｍオブジェクトは、エラーまたはタイムアウトが生じる場合に、認証プロセスが一旦完了すると破壊される。本発明の認証オブジェクトについて、下記で説明する。

【００４３】

（ｃ．認証オブジェクト）

認証オブジェクトも、それぞれの新しいクライアントセッションに関して具現化される。認証オブジェクトのタスクが図８に示される。図８において、ステップ８０２から制御が始まる。ステップ８０２において、認証オブジェクトは、ユーザを認証するために使用される方針（または、方針オブジェクト）をデータベース（または、データベースオブジェクト）から検索する。その後、制御はステップ８０４に移動する。

【００４４】

ステップ８０４において、認証オブジェクトは、次いで、ウェブブラウザ２１２と通信するために必要とされる全ての必要なメッセージの（フィルタ２０６および認証制御コンポーネント２０８を介する）交換を管理する。認証メッセージの交換が一旦完了すると、制御はステップ８０６に移動する。

【００４５】

ステップ８０６において、認証オブジェクトは、最終的な結果をフィルタ２０

６に返し、フィルタ２０６は、今度は、サーバ／ウェブアプリケーション２１４とインターラクトして、ユーザとのアクセスを可能（または、不可能）にする。フィルタ２０６とサーバ／ウェブアプリケーション２１４との間でインターラクトして、ユーザとのアクセスの制御を引き渡すことは、本発明によって、インテグレーション（ｉｎｔｅｇｒａｔｉｏｎ）と呼ばれる。図８のフローチャートは、この時点で終了する。本発明のクライアント側コンポーネントについて、下記で説明する。

【００４６】

（２．クライアント側コンポーネント）

認証制御コンポーネント２０８は、デバイス特有のコンポーネント２１０およびウェブブラウザ２１２と共に、本発明によって、クライアント側コンポーネントとして分類される。デバイス特有のコンポーネント２１０は、ソフトウェアライブラリおよび識別デバイス（例えば、指紋スキャナ、音声または顔面識別システムなどのバイオメトリックデバイス、あるいは、ＲＳＡトークン、ＶＡＳＣＯトークンなどの安全トークンなど）特有の他のコンポーネントである。デバイス特有のコンポーネント２１０は、典型的には、デバイスの製造者によって出荷され、通常、デバイスとインタフェースするために使用され得るアプリケーションプログラミングインタフェース（ＡＰＩ）を含む。ＡＰＩは、関連分野で周知である。

【００４７】

認証制御コンポーネント２０８は、デバイス特有のコンポーネント２１０と共に作用して、必要な任意のローカル処理を行い、この処理の結果をフィルタ２０６に伝えることにより、ユーザ信用証明書を取り込むプロセスを管理する。例えば、認証制御コンポーネント２０８は、特定のウェブブラウザ（例えば、インターネットエクスプローラ）に関してＡｃｔｉｖｅＸ制御として実施され得、他のウェブブラウザ（例えば、ネットスケープ）に関するＡｃｔｉｖｅＸ制御と同じ論理を含むプラグインとして実施され得る。

【００４８】

本発明のクライアント側コンポーネントは、ソフトウェアの保全性および一度

だけのダウンロードを含む２つの機能を提供する。認証制御コンポーネント２０８がクライアントコンピュータまたは装置に一旦ダウロードされると、悪意のあるユーザは、認証制御コンポーネント２０８を不正変更し得る。これを防止するために、認証制御コンポーネント２０８が使用される前のそれぞれの場合に、クライアントソフトウェアの保全性が調べられる。これは、認証制御コンポーネント２０８に関するコード、および、デバイス特有のコンポーネント２１０に関するコードをハッシングすることにより達成され得る。任意の変更が発見されると、次いで、認証制御コンポーネント２０８および／またはデバイス特有のコンポーネント２１０に関する本来のコードが、本発明の認証が続行される前にダウンロードされる。

【００４９】

本発明の一度だけのダウンロード機能は、登録の時、または、ユーザが認証制御コンポーネント２０８を有さないコンピュータから認証を試みる最初の時のいずれかの場合に、ユーザのコンピュータに、特定のバージョンの認証制御コンポーネント２０８が一度だけダウンロードされるという事実に対処する。その後、それぞれの新しいバージョンの認証制御コンポーネント２０８も、ユーザのコンピュータに一度だけダウンロードされる。フィルタコンポーネントについて、下記で説明する。

【００５０】

（３．フィルタコンポーネント）

フィルタ２０６は、ウェブ／アプリケーションサーバ２１４にある軽量のコンポーネント（すなわち、本発明の認証サービスを必要とする任意のウェブサーバまたはアプリケーションサーバ）である。フィルタ２０６に関するコードは、好適には、最適な性能のために、ウェブ／アプリケーションサーバ２１４のネイティブ言語（例えば、Ｃ、Ｃ＋＋、Ｊａｖａ（Ｒ）など）によって書かれる。本発明の一実施形態において、フィルタ２０６は、ウェブブラウザ２１２から送信された全てのリクエストを調べて、認証に関する任意のリクエストをウェブブラウザ２１２から妨害する。その後、フィルタは、認証リクエストを認証サーバ２０２に転送する。

【００５１】

フィルタ２０６は、既存のウェブサーバ（ネットスケープエンタープライズサーバ（ＮＥＳ）、マイクロソフトインターネットインフォメーションサーバ（ＭＳＩＳ）、アパッチなどを含むが、これらに制限されない）と相互に機能し合って、ウェブサイトにアクセスするための認証サービスを提供するように設計される。フィルタ２０６は、さらに、アプリケーションサーバ（ＢＥＡのウェブ論理、シルバーストリームのアプリケーションサーバ、オラクルのＡｐｐサーバ、サンのネットダイナミックス、マイクロソフトのサイトサーバなどを含むが、これらに制限されない）によって使用されて、ウェブアプリケーション（オンラインバンキング、オンライン株式取引などを含む）のための認証サービスを提供し得る。図２に示すように、フィルタ２０６は、ウェブ／アプリケーションサーバ２１４に接続される。ウェブ／アプリケーション４１２は、上記のように、ウェブサーバおよびアプリケーションサーバの両方を表す。本発明の遠隔登録コンポーネントについて、下記で説明する。

【００５２】

（４．遠隔登録コンポーネント）

本発明は、ユーザが、それぞれの信用証明書を（インターネット、イントラネット、無線ネットワークなどを介して）遠隔的に登録することを可能にする。本発明の遠隔登録コンポーネントは、認証制御コンポーネント２０８、認証コンポーネント２０４、および中間層（ｍｉｄｄｌｅ－ｔｉｅｒ）登録アプリケーションを含む。上記のように、認証制御コンポーネント２０８は、登録および認証（クライアント側コンポーネント）にも使用され得る。認証コンポーネント２０４は、ｌｉｓｔｅｎオブジェクト、ｃｏｍｍオブジェクト、および登録オブジェクト（上記の認証オブジェクトの対の片方）を含む。これにより、登録の時、または、ユーザが登録したコンピュータとは異なるコンピュータに移動する場合、ユーザがその異なるコンピュータから認証を試みる最初の時のいずれかの場合に、認証制御コンポーネント２０８の「一度だけ」のダウンロードが可能になる。さらに、認証コンポーネント２０４を使用して、登録および認証（サーバ側コンポーネント）が行われ得る。

【００５３】

本発明の遠隔登録機能は、ユーザの信用証明書（例えば、バイオメトリック測定、パスワードなど）を取り込み、信用証明書を登録オブジェクトに送信して、本発明によるユーザの未来の認証のために認証サーバ２０２のデータベース内に格納するために、認証制御コンポーネント２０８を必要とする。

【００５４】

登録アプリケーションは、遠隔登録プロセスの提示論理を駆動させる。登録アプリケーションは、ウェブブラウザ２１２内に表示するユーザに可視のＨＴＭＬを作成する責任がある。いくつかの技術を使用して、ユーザに可視のＨＴＭＬ（アクティブサーバページ（ＡＳＰ）、Ｊａｖａ（Ｒ）サーバページ（ＪＳＰ）、ＪＡＶＡ（Ｒ）サーブレット、マイクロソフトＩＳＡＰＩ、およびネットスケープＮＳＡＰＩを含むが、これらに制限されない）が実施され得る。登録アプリケーションは、一方で、仲介役の認証制御コンポーネント２０８として機能し、他方で、ｌｉｓｔｅｎオブジェクト、ｃｏｍｍオブジェクト、および登録オブジェクトとして機能する。ｌｉｓｔｅｎオブジェクト、ｃｏｍｍオブジェクト、および登録オブジェクトのタスクについて、下記で説明する。

【００５５】

（ａ．ｌｉｓｔｅｎオブジェクト）

上記のように、ｌｉｓｔｅｎオブジェクトは、認証サーバ２０２が起動する際に認証サーバ２０２によって具現化される。ｌｉｓｔｅｎオブジェクトは、図９に示すように、下記のタスクを行う責任がある。図９において、フローチャートがステップ９０２から始まる。一旦具現化されると、ｌｉｓｔｅｎオブジェクトは、ステップ９０２によって示すように、標準ＳＳＬポート（すなわち、ポート４４３）で入来するＳＳＬ接続リクエストをリッスンするＨＴＴＰデーモンのように機能する。その後、制御はステップ９０４に移動する。

【００５６】

ステップ９０４において、ｌｉｓｔｅｎオブジェクトがＳＳＬ接続リクエストを一旦受信すると、ｌｉｓｔｅｎオブジェクトは、リクエストのパラメータを調べて、登録オブジェクト、ｃｏｍｍオブジェクト、または本発明が支持する任意

の他の機能オブジェクトのいずれに制御が移動されるべきかを決定する。図６が、１つのタイプのリクエストだけ（すなわち、認証リクエスト）が可能である場合を示すことに留意されたい。その後、制御はステップ９０６に移動する。

【００５７】

ステップ９０６において、ｌｉｓｔｅｎオブジェクトは、リクエストが処理されることを保証する。その後、制御はステップ９０２に戻り、ここで、ｌｉｓｔｅｎオブジェクトは、入来するＳＳＬ接続リクエストをリッスンする。ｌｉｓｔｅｎオブジェクトが破壊されるのは、認証サーバ２０２がオフになってからのみである。

【００５８】

（ｂ．ｃｏｍｍオブジェクト）

ｃｏｍｍオブジェクトは、それぞれの新しいクライアントセッションに関して具現化される。クライアントセッションは、ウェブブラウザ２１２におけるユーザが、ウェブ／アプリケーションサーバ２１４にアクセスしようと試みる場合に生じる。登録プロセスが一旦完了すると、エラーまたはタイムアウトが生じて、対応するｃｏｍｍオブジェクトが破壊される。ｃｏｍｍオブジェクトは、図７によって示すタスクと同じタスクを行う責任がある。

【００５９】

（ｃ．登録オブジェクト）

登録オブジェクトは、論理を実施する点と、認証制御コンポーネント２０８との（登録アプリケーションを介した）メッセージ交換を駆動する点とにおいて、上記の認証オブジェクト対の片方である。各新規クライアントセッションにおいても、登録オブジェクトの新規インスタンスをインスタンス化する。登録オブジェクトのタスクを図１０に示す。図１０において、制御は工程１００２から開始する。工程１００２において、登録オブジェクトは、当該ユーザについて方針（または方針オブジェクト）を生成する。その後、制御は工程１００４へと進む。

【００６０】

工程１００４において、生成された方針に基づいて、登録オブジェクトは、必要な信用証明書をユーザにリクエストする。この信用証明書はテンプレートとし

て保存される。例えば、方針がユーザを指紋デバイスおよび手形デバイスの両方にかけることを要求する場合、登録オブジェクトは、ユーザの指紋および手形のバイオメトリック測定値をリクエストする。その後、制御は工程１００６に進む。

【００６１】

工程１００６において、登録オブジェクトは、認証サーバ２０２のデータベース中に方針および信用証明書（またはテンプレート）を格納する。この時点で、図１０のフローチャートは終了する。

【００６２】

本発明の実施形態は、上述した本発明の機能コンポーネントを全て含むが、上述したような本発明の範囲内に各コンポーネントの機能がある限り、複数の（または全ての）コンポーネントを組み合わせても良い。

【００６３】

（Ｃ．本発明の例示的インプリメンテーション）

（１．例示的環境）

認証サーバ２０２、認証コンポーネント２０４、フィルタ２０６、認証制御コンポーネント２０８、登録ステーション、管理ステーションおよび衛星登録ステーションを、図３に示すようなコンピュータ３００を用いてインプリメントすることが可能である。これらの機能コンポーネントのうち１つ以上を単一のコンピュータ３００上でインプリメントすることが可能であることは明らかである。

【００６４】

本発明は、ハードウェア、ソフトウェアまたはこれらの組み合わせを用いてインプリメント可能であり、コンピュータシステムまたは他の処理システム中でインプリメントすることも可能である。実際、一実施形態において、本発明は、本明細書中に記載の機能性を実施することが可能な１つ以上のコンピュータシステムに関する。コンピュータシステム３００は、１つ以上のプロセッサ（例えば、プロセッサ３０４）を含む。プロセッサ３０４は、通信バス３０６に接続される。様々なソフトウェア実施形態について、この例示的コンピュータシステムを用いて説明する。当業者にとって、以下の記載を読めば、他のコンピュータシステ

ムおよび／またはコンピュータアーキテクチャを用いて本発明をインプリメントする方法は明らかである。

【００６５】

コンピュータシステム３００は主メモリ３０８（好適にはランダムアクセスメモリ（ＲＡＭ）も含み、二次メモリ３１０も含む。二次メモリ３１０は、例えば、ハードディスクドライブ３１２および／またはリムーバブル格納ドライブ３１４（これは、フロッピー（Ｒ）ディスクドライブ、磁気テープドライブ、光学ディスクドライブなどを表す）を含み得る。リムーバブル格納ドライブ３１４は、リムーバブル格納ユニット３１８に対する読出しおよび／または書込みを周知の方法で行う。リムーバブル格納ユニット３１８は、リムーバブル格納ドライブ３１４による読出しおよび書込みの対象となるフロッピー（Ｒ）ディスク、磁気テープ、光学ディスクなどを表す。理解されるように、リムーバブル格納ユニット３１８は、コンピュータソフトウェアおよび／またはデータが内部に格納されたコンピュータによる利用が可能な格納媒体を含む。

【００６６】

別の実施形態において、二次メモリ３１０は、コンピュータプログラムまたは他の命令をコンピュータシステム３００にロードすることを可能にする他の類似する手段を含み得る。このような手段を挙げると、例えば、リムーバブル格納ユニット３２２およびインターフェース３２０がある。このような例示的手段は、プログラムカートリッジおよびカートリッジインターフェース（例えば、映像ゲームデバイスにおいて見受けられるようなもの）と、リムーバブルメモリチップ（例えば、ＥＰＲＯＭまたはＰＲＯＭ）および関連付けられたソケットと、ソフトウェアおよびデータをリムーバブル格納ユニット３１８からコンピュータシステム３００に転送することを可能にする他のリムーバブル格納ユニット３２２およびインターフェース３２０とを含み得る。

【００６７】

コンピュータシステム３００はまた、通信インターフェース３２４も含み得る。通信インターフェース３２４により、コンピュータシステム３００と外部デバイスとの間でソフトウェアおよびデータを転送することが可能となる。通信イン

ターフェース３２４の例を挙げると、モデム、ネットワークインターフェース（例えば、イーサネット（R）カード）、通信ポート、ＰＣＭＣＩＡスロットおよびカードなどがある。通信インターフェース３２４を介して転送されるソフトウェアおよびデータは信号の形態をとり、信号の形態の例を挙げると、通信インターフェース３２４による受信が可能な電子信号、電磁気信号、光学信号または他の信号がある。これらの信号３２６は、チャンネル３２８を介して通信インターフェースに提供される。このチャンネル３２８は、信号３２６を搬送し、ワイヤまたはケーブル、光ファイバ、電話線、セルラー電話リンク、ＲＦリンクおよび他の通信チャンネルを用いてインプリメント可能である。

【００６８】

本文書中、「コンピュータプログラム媒体」および「コンピュータによる利用が可能な媒体」という用語を、リムーバブル格納デバイス３１８、ハードディスクドライブ３１２にインストールされたハードディスク、および信号３２６などの媒体を主に指すものとして用いる。これらのコンピュータプログラム製品は、ソフトウェアをコンピュータシステム３００に提供する手段である。

【００６９】

コンピュータプログラム（コンピュータ制御論理とも呼ばれる）は、主メモリおよび／または二次メモリ３１０に格納される。通信インターフェース３２４を介してコンピュータプログラムを受信してもよい。このようなコンピュータプログラムは、実行されると、コンピュータシステム３００をイネーブルして、本明細書中にて説明したような本発明の機能を行わせる。詳細には、コンピュータプログラムは、実行されると、プロセッサ３０４をイネーブルして、本発明の機能を行わせる。よって、このようなコンピュータプログラムは、コンピュータシステム３００の制御器を表す。

【００７０】

本発明の実施構成をソフトウェアを用いて行う実施形態において、ソフトウェアをコンピュータプログラム製品に格納し、リムーバブル格納ドライブ３１４、ハードドライブ３１２または通信インターフェース３２４を用いてコンピュータシステム３００にロードすることが可能である。制御論理（ソフトウェア）は、

プロセッサ３０４によって実行されると、本明細書中に記載の本発明の機能をプロセッサ３０４に行わせる。

【００７１】

別の実施形態において、本発明は、例えば、ハードウェアコンポーネント（例えば、特定用途向け集積回路（ＡＳＩＣ））を用いる主にハードウェアにおいて実施される。本明細書中に記載の機能を行うためのハードウェア状態マシンのインプリメンテーションは、当業者（単数または複数）にとって明らかである。さらに別の実施形態において、本発明は、ハードウェアおよびソフトウェアの両方を組み合わせて実施される。

【００７２】

（２．例示的ネットワークアーキテクチャおよびプログラミング言語）

上述したように、コンピュータプログラムは、実行されると、コンピュータ３０２をイネーブルして、本明細書中に記載の本発明の機能を行わせる。一実施形態において、本発明の実施構成を、オブジェクト指向プログラミング言語で書かれたコンピュータプログラムを用いて行う。オブジェクト指向プログラミングは、データ構造のデータの種類だけではなく、当該データ構造に適用することが可能な動作（機能）の種類もプログラマによって規定される一種のプログラミングである。このようにして、データ構造を、データおよび機能の両方を備えたオブジェクトとする。加えて、プログラマは、あるオブジェクトと別のオブジェクトとの間の関係も生成することができる。例えば、オブジェクトは、他のオブジェクトの特性を受け継ぐことができる。

【００７３】

命令型プログラミング技術と比較してオブジェクト指向プログラミング技術が有利である１つの理由として、オブジェクト指向プログラミング技術では、プログラマが、新種のオブジェクトが追加された際に変更を行う必要が無いモジュールを作成することが可能であることがある。プログラマが新規オブジェクトを生成するだけで、当該オブジェクトは既存のオブジェクトから多くの特徴を受け継ぐ。そのため、オブジェクト指向プログラムは改変が容易なものとなっている。オブジェクト指向プログラミングを行う場合、オブジェクト指向プログラミング

言語（ＯＯＰＬ）が必要となる。Ｃ＋＋およびＳｍａｌｌｔａｌｋの２つはその中でも特に一般的な言語であり、Ｐａｓｃａｌのオブジェクト指向版もある。

【００７４】

本発明の実施形態の実施構成をオブジェクト指向プログラミング言語で書かれたコンピュータプログラムを用いて行っているが、本発明の実施構成は命令型プログラミング言語などを用いても行うことが可能である。

【００７５】

上述したように、１つ以上のコンピュータ３０２をネットワークによって接続する。本発明の実施形態では、ピアツーピアオブジェクトアーキテクチャと呼ばれる種類のネットワークアーキテクチャを用いる。ピアツーピアオブジェクトアーキテクチャの説明に入る前に、クライアント／サーバアーキテクチャと呼ばれる種類のネットワークアーキテクチャについて説明する必要がある。クライアント／サーバアーキテクチャは、ネットワーク上の各コンピュータまたはプロセスをクライアントまたはサーバとして扱うネットワークアーキテクチャである。サーバは、ディスクドライブ（ファイルサーバ）、プリンタ（プリントサーバ）、アプリケーション／機能またはネットワークトラフィック（ネットワークサーバ）の管理のみを行うコンピュータまたはプロセスである。実際、サーバは、アプリケーション用リソースを割り当てる任意のコンピュータまたはデバイスである。クライアントは、ユーザによるアプリケーション実行が行われるパーソナルコンピュータまたはワークステーションである。クライアントは、自身のリソース（例えば、ファイル、デバイス、機能の実行およびさらには処理能力）をサーバに依存する。

【００７６】

上述したように、本発明の実施形態では、ピアツーピアオブジェクトアーキテクチャと呼ばれる種類のネットワークアーキテクチャを用いる。ピアツーピアオブジェクトアーキテクチャは、ネットワーク中の各コンピュータが同様の能力および責任を有する状態である。このような状態は、一部のコンピュータを残りのコンピュータのみに対して機能させるクライアント／サーバアーキテクチャと異なる。そのため、本発明の実施形態において、コンピュータ３０２は全て、サー

バまたはクライアントのどちらとしても動作することができる。次に、認証サーバ２０２中に格納されるエンジンおよびデータについて説明する。

【００７７】

（Ｄ．本発明のエンジンおよびデータ）

上述したように、図２の認証サーバ２０２は、本発明のエンジンである。本発明の実施形態において、（方針を実行する）このエンジンは、ユーザを本発明によって認証すべきか否かを最終決定する。さらに、認証サーバ２０２は、本発明によってアクセスされるデータを格納する。認証サーバ２０２中に格納されたデータを構成可能にする方法としては、当該データをデータベースおよびディレクトリを構成するものとして構成する方法がある。データベースの構成およびディレクトリの構成のいずれについても、同時係属中の関連米国出願第０９／２６４，７２６号および米国出願第０９／５１７，１２１号に詳細な記載がある。

【００７８】

認証サーバ２０２に格納された様々なデータの収集と、アドミニストレータが認証サーバ２０２を初期設定する際に用いることの多い一連の工程とについても、本発明と関連する同時係属中の米国出願第０９／２６４，７２６号および米国出願第０９／５１７，１２１号に詳細な記載がある。認証サーバ２０２に格納されることの多いデータを挙げると、テンプレート、方針、グループ、デバイスＩＤ、ユーザＩＤ、コンピュータＩＤおよびアプリケーションＩＤがある（ただし、これらに限定されない）。

【００７９】

ユーザが異なる識別デバイスに登録するたびに、１つ以上の一意に定まるテンプレートが生成され、認証サーバ２０２に格納される。テンプレートは、特定のバイオメトリックデバイス用のユーザの一意に定まる測定値（これは、その後、バイオメトリックデバイスがユーザ識別を試行する際、当該テンプレートと、ユーザの「ライブ」測定値とをマッチングさせる際に用いられる）を格納するか、または、非バイオメトリックデバイスの場合はパスワードなどを格納する。

【００８０】

本発明の方針は、認証サーバ２０２によってユーザを認証する方法または様式

を決定するものである。本発明によって与えられる事前規定された方針の具体例を挙げると、ＯＲ方針、ＡＮＤ方針、ＣＯＮＴＩＮＧＥＮＴ方針、ＲＡＮＤＯＭ方針、閾値方針、複数のユーザ方針、複数の位置方針、マルチテンプレート方針、ユーザ依存方針、位置限定方針、およびコンピュータ／デバイス特定方針がある。本発明ではまた、アドミニストレータが他の方針を規定または構成することも可能である。上記の方針については、本発明に関連する同時係属中の米国出願第０９／２６４，７２６号および米国出願第０９／５１７，１２１号に詳細な記載がある。

【００８１】

各事前規定された方針には、各方針と関連付けられたデバイスのリストがある。このデバイスリストにより、特定の方針を実行する際に用いられる識別デバイスを識別する。デバイスリスト中の各デバイスには、各デバイスと関連付けられた閾値および時間切れ値（このような値は、バイオメトリックデバイスの場合に用いられることが多い）が設けられ得る。閾値（例えば、誤採択率）が示すのは、デバイスがユーザを当該デバイスから先に通過させるべきか否か判定する際の識別レベルである。時間切れ値が示すのは、デバイスがユーザ識別を閾値が示す識別レベルまで行わなければならない時間の枠である。

【００８２】

本発明におけるグループは、ウェブ／アプリケーションサーバ２１４に格納された一連の同一情報へのアクセスを必要とする１つ以上のユーザを論理的に組み合わせる方法である。例えば、インターネットを用いている全ユーザに、株式取引を可能にするオンラインアプリケーションのログインページへのアクセスを許可し得る。そして、同じオンラインアプリケーションについて、ユーザと、当該ユーザが指定した他のユーザのみとを、当該ユーザの秘匿情報へのアクセスが認められたグループに加える。これにより、これらのグループのうち１つのグループを「ＵＳＲ２４４５８グループ」として規定することができる。ここで、あるユーザが「ＵＳＲ２４４５８グループ」に加えられると、そのユーザは、（本発明による認証を受けた後に）「ＵＳＲ２４４５８グループ」に所属する他のユーザ全員が用いるリソースと同じリソースにアクセスする。

【００８３】

各ユーザを、１つ以上のグループに加えることが可能である。ユーザが特定のグループ中の情報へのアクセスを得ようとする場合、そのユーザは、その特定のグループに関連付けられている方針がどのようなものであれ、その方針による認証を受けなければならない。

【００８４】

デバイスＩＤは、識別デバイスを識別するものである。各識別デバイスには一意に定まるＩＤがある。そのため、本発明では、このようなデバイスＩＤの収集により、通信プロトコルによってイネーブルされる（インターネット内の）クライアント（ウェブブラウザ）に取り付けられた各識別デバイスを、一意に定まった様式で識別することが可能となる。同様に、ユーザＩＤにより、本発明を利用するユーザを一意に定まった様式で識別する。次に、セクションＥおよびセクションＦそれぞれにおいて、ユーザの認証およびユーザの遠隔登録の際の本発明のコンポーネント間のメッセージフローについて説明する。

【００８５】

（Ｅ．本発明による認証の際のコンポーネント間のメッセージフロー）

図１１は、本発明の実施形態に従ってウェブブラウザ２１２を用いるユーザを認証するための本発明のコンポーネント間の高レベルのメッセージフローを示す。本発明のサービスを用いたウェブサイトまたはウェブアプリケーションにユーザがアクセスしようとすると、当該ユーザは、当該ユーザが登録プロセスの間に登録した「ユーザ名」（またはユーザを識別する任意の一意に定まるユーザＩＤ）を入力するようプロンプトされる。この「ユーザ名」は、フローライン１１０２に示すようにフィルタ２０６に送られる。

【００８６】

フィルタ２０６は、「ユーザ名」を受信すると、フローライン１１０４に示すように、認証サーバ２０２のデータベースに格納されている「ユーザ名」の方針およびテンプレート（または信用証明書）を取得したいとの旨のリクエストを認証サーバ２０２に（認証コンポーネント２０４を介して）送る。

【００８７】

認証サーバ２０２は、フローライン１１０６に示すように、「ユーザ名」方針およびテンプレートを取得し、取得された「ユーザ名」方針およびテンプレートをフィルタ２０６に（認証コンポーネント２０４を介して）返送する。

【００８８】

これらの方針およびテンプレートに基づいて、フィルタ２０６は、フローライン１１０８に示すように、ユーザの信用証明書を提示するようユーザに呼びかける。ここで、認証制御コンポーネント２０８は、必要な任意のバイオメトリック測定値の取得プロセスおよびマッチングプロセスを通じてユーザを先導する。

【００８９】

その後、フローライン１１１０および１１１２にそれぞれ示すように、認証制御コンポーネント２０８は、フィルタ２０６による呼びかけの結果を送る。フィルタ２０６は、上記結果を認証サーバ２０２に（認証コンポーネント２０４を介して）転送する。

【００９０】

その後、認証サーバ２０２は、ユーザ方針に基づいて、マッチング結果が満足できるものであるか否かと、（多元認証または多元方針の場合のように）信用証明書がさらに必要か否かとを判定して、当該ユーザがリクエストした特定の情報にアクセスする。多元認証が必要な場合、フローライン１１０６～１１１２を必要な限り何回も繰り返す。

【００９１】

認証サーバがユーザ方針を実行できるようになり、当該ユーザが認証されているか否かを判定すると、認証コンポーネント２０４は、フローライン１１１４に示すように、判定結果をフィルタ２０６に転送する。ここで、ユーザが認証されると、フィルタ２０６はウェブ／アプリケーションサーバ２１４とインターラクトして、ユーザがそのリクエストされた情報にアクセスすることを許可する。

【００９２】

ユーザは、当該セッションが継続する間（すなわち、ユーザがウェブブラウザ２１２を閉鎖するまで）ウェブアプリケーションまたはウェブサイトを利用することができる。そのため、フィルタ２０６は、フローライン１１１６に示すよう

に、ユーザがリクエストされた情報にアクセスすることを許可するかまたは拒否する。次に、本発明の遠隔登録を行うためのコンポーネント間のメッセージフローについて説明する。

【００９３】

（Ｆ．本発明の遠隔登録を行うためのコンポーネント間のメッセージフロー）

図１２は、ウェブブラウザ２１２を用いるユーザを本発明の実施形態に従って遠隔登録するための本発明のコンポーネントの間の高レベルメッセージフローを示す。遠隔登録に用いられるメッセージフローは、認証に用いられるメッセージフローと極めて類似する。登録アプリケーションは、ユーザとの対話を管理するものである。本発明では、ユーザが登録アプリケーションそのものを利用する行為を認証する際、複数の技術を用いることが可能である。例えば、ユーザが現在アプリケーションまたはウェブサイトにアクセスする際に用いている既存のユーザ名とパスワードとの組み合わせを用いてもよい。別の例として、一回のみ利用される（ｏｎｅ－ｔｉｍｅ）パスワードまたはＰＩＮを生成して、ユーザに（電子的にまたは他の方法で）送ってもよい。いずれの場合にも、登録オブジェクト（これについては、図１０を参照して説明した）は、一回のみ利用される認証をユーザに行った後、ユーザのコンピュータ上にある認証制御コンポーネント２０８をダウンロードする。

【００９４】

図１２を参照して、ユーザは、フローライン１２０２に示すように、一回のみ利用されるパスワードまたはＰＩＮをフィルタ２０６に提出する。

【００９５】

その後、フィルタ２０６は、フローライン１２０４に示すように、ユーザの一回のみ利用される認証を登録オブジェクト別にリクエストする。

【００９６】

一回のみ利用される認証の結果は、フローライン１２０６に示すようにフィルタ２０６に返送される。

【００９７】

フィルタ２０６は、フローライン１２０８に示すように、このリクエストを認

証制御コンポーネント２０８に転送する。

【００９８】

認証制御コンポーネント２０８は、フローライン１２１０に示すように、必要なバイオメトリック測定値をユーザから（登録アプリケーションを介して）取得し、その後、この取得結果をフィルタ２０６に送る。

【００９９】

次いで、フローライン１２１２に示すように、この取得結果をフィルタ２０６から登録オブジェクトに転送して、認証サーバ２０２に格納する。この時点において、ユーザは、本発明において登録される。次に、本発明のコンポーネントＡＰＩおよび拡張性について説明する。

【０１００】

（Ｇ．本発明のコンポーネントＡＰＩおよび拡張性）

サーバ側コンポーネント（すなわち、認証サーバ２０２および認証コンポーネント２０４）、フィルタ２０６ならびに登録アプリケーションは、ウェブによってイネーブルされるクライアントに良好に規定されたインターフェースを提示する。これらのインターフェースは、ＨＴＴＰ　ＧＥＴ方法またはＰＯＳＴ方法を用いてリクエストすることが可能な一連のＵＲＬからなる。以下に示すＡＰＩおよび関連規約は、これらの対話をインプリメントする方法の一例に過ぎない。下記の例は本発明を限定することを意図したものではない。全てのＵＲＬリクエストに対し、以下のシンタックスに従うように要求することができる。

ＭＥＴＨＯＤ　ＨＴＴＰ法の種類。ＧＥＴまたはＰＯＳＴであり得る。

ＨＥＡＤＥＲＨＴＴＰ　ＨＴＴＰヘッダ。フォーマットは名＝値。

ＢＯＤＹ　ＨＴＴＰリクエストボディ。複数の名＝値対、バイナリデータ、またはこれらの両方であり得る。

＜ｆｏｏｂａｒ＞　Ｄオプションのエレメントを示す。

ｆｏｏ｜ｂａｒ　「ｆｏｏ」ＯＲ「ｂａｒ」を示す。

【０１０１】

サーバ側コンポーネント、フィルタ２０６および登録アプリケーションは、リクエストが特定のフォーマットになっていることを予測する。これらのリクエス

トに対する応答もまた、特定のフォーマットに準拠する。これにより、拡張性のあるアーキテクチャが得られ、また、ウェブによってイネーブルされる新規サービスが既存インフラストラクチャにプラグインすることが可能となる。ＢＮＦは「Ｂａｃｋｕｓ－Ｎａｕｒ　Ｆｏｒｍ」の頭字語であり、これは、プログラミング言語、コマンドセットなどのシンタックスを指定する際に用いられるメタシンタクチック表記である。以下は、本発明のリクエストのＢＮＦであり、これは、生成しなければならないオブジェクトの種類の識別情報と、オブジェクトに送られるデータとを含む。

【０１０２】

【数１】

<request> ::= <function> | <request><connector><request>

<function> ::= <identifier> ({<parameter>})

<parameter> ::= <identifier> | <identifier>

<identifier> ::= <letter> {<letter> | <digit>}

<letter> ::= **A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z**

<digit> ::= **0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9**

<connector> ::= **AND |**
OR

上記の方法と同じ方法を用いて、複数のＵＲＬが異なる場合にも、本アーキテクチャを容易に伸展して、他のウェブ機能性を認証サーバ２０２に追加することが可能である。このような別の機能性の例としては、認証サーバ２０２の遠隔管

理がある。

【０１０３】

（H．結論）

上記にて本発明の様々な実施形態について説明してきたが、上記の実施形態は例示目的のために示したものであって限定目的のためのものではないことが理解されるべきである。上記実施形態の様態および詳細には、本発明の趣旨および範囲から逸脱することなく様々な変更を為すことが可能であることが可能であることは、当業者にとって明らかである。これは、今後開発される関連分野（単数または複数）における技術および状況を鑑みれば自明である。よって、本発明は上記の例示的実施形態のいずれによっても限定されるべきものではなく、本明細書中の特許請求の範囲およびその均等物のみによって規定されるべきである。

【図面の簡単な説明】

【図１】

図１は、インターネットに接続された複数のクライアントおよびサーバを示すネットワークブロック図である。

【図２】

図２は、１実施形態によって、本発明の例示的な動作環境を表すブロック図である。

【図３】

図３は、１実施形態によって、本発明のコンポーネントを実施するために使用され得る例示的なコンピュータを示す。

【図４】

図４は、本発明の１実施形態によって、通信プロトコルが無線通信プロトコルである場合に必要とされる機能を実行する認証コンポーネントを示す。

【図５Ａ】

図５Ａは、本発明の１実施形態によって、通信プロトコルがローカルネットワークまたはイントラネット用である場合に必要とされる機能を実行する認証コンポーネントを示す。

【図５Ｂ】

図５Ｂは、本発明の１実施形態によって、通信プロトコルがインターネット用である場合に必要とされる機能を実行する認証コンポーネントを示す。

【図６】

図６は、本発明の１実施形態による認証機能のｌｉｓｔｅｎオブジェクトのタスクを示す。

【図７】

図７は、本発明の１実施形態による認証機能のｃｏｍｍオブジェクトのタスクを示す。

【図８】

図８は、本発明の１実施形態による認証機能の認証オブジェクトのタスクを示す。

【図９】

図９は、本発明の１実施形態による遠隔登録機能のｌｉｓｔｅｎオブジェクトのタスクを示す。

【図１０】

図１０は、本発明の１実施形態による遠隔登録機能の登録オブジェクトのタスクを示す。

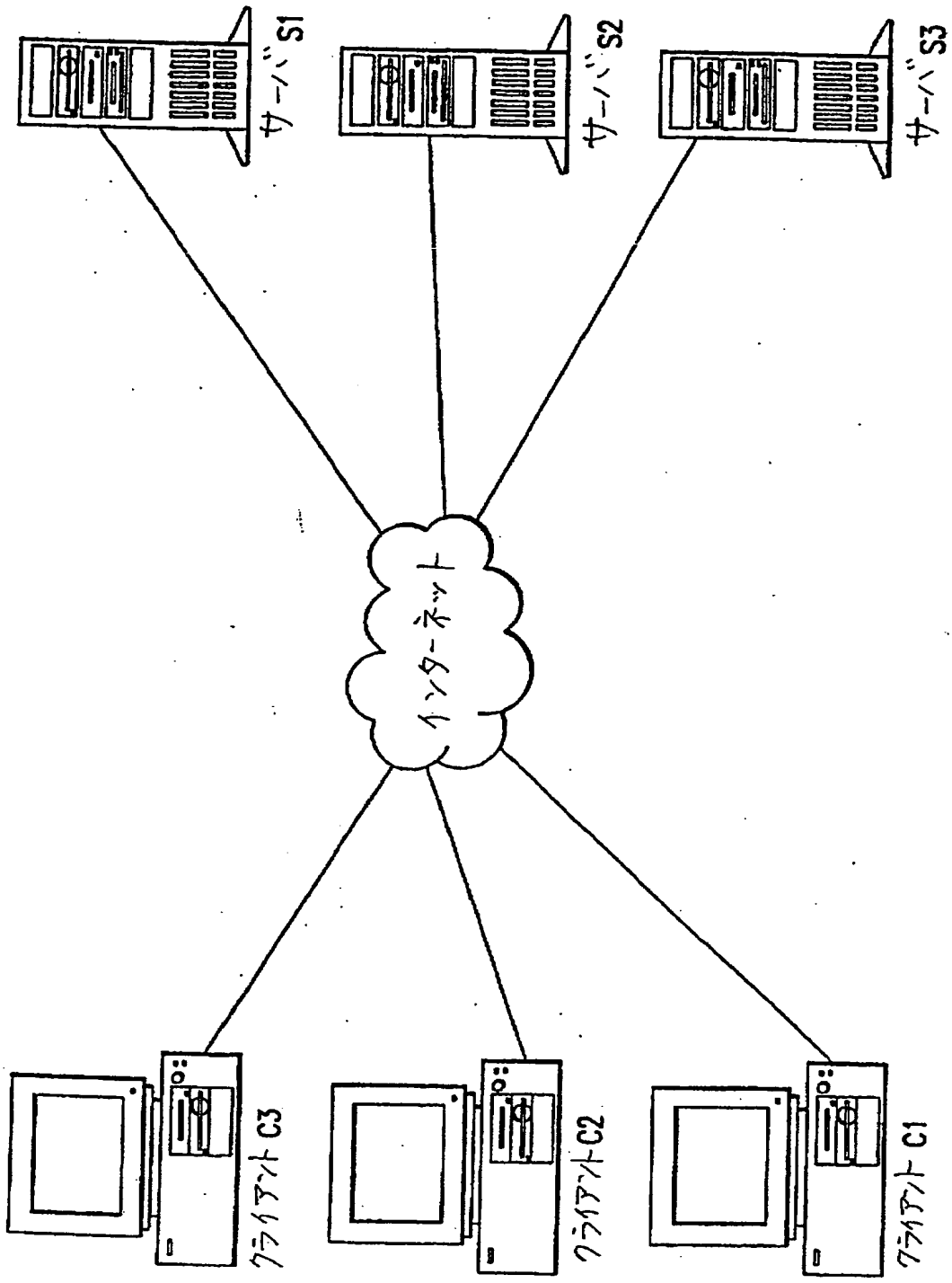
【図１１】

図１１は、本発明の１実施形態によって、ウェブブラウザを使用してユーザを認証するための本発明のコンポーネント間の高レベルメッセージフローを示す。

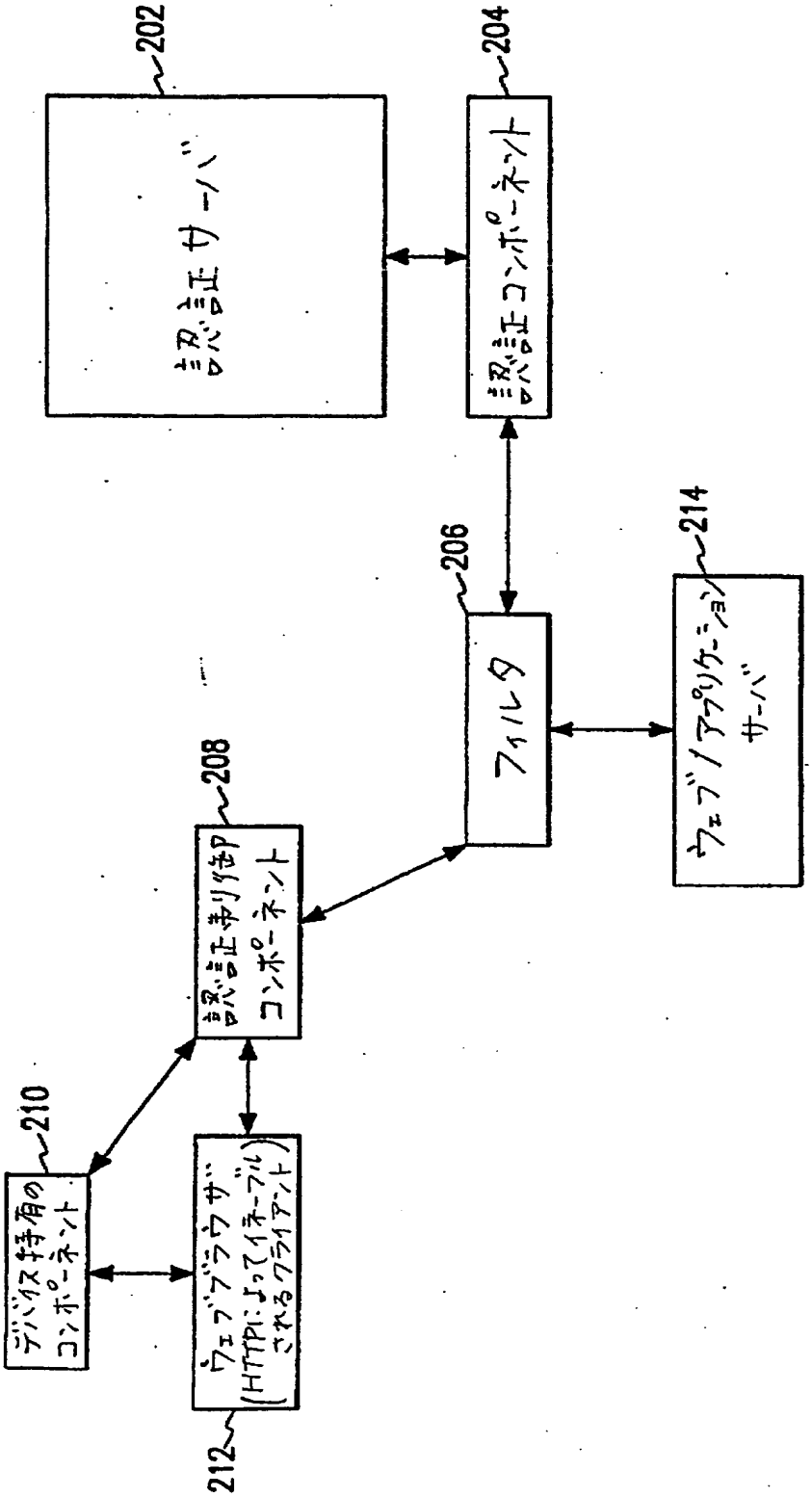
【図１２】

図１２は、本発明の１実施形態によって、ウェブブラウザ２１２を使用してユーザを遠隔登録するための本発明のコンポーネント間の高レベルメッセージフローを示す。

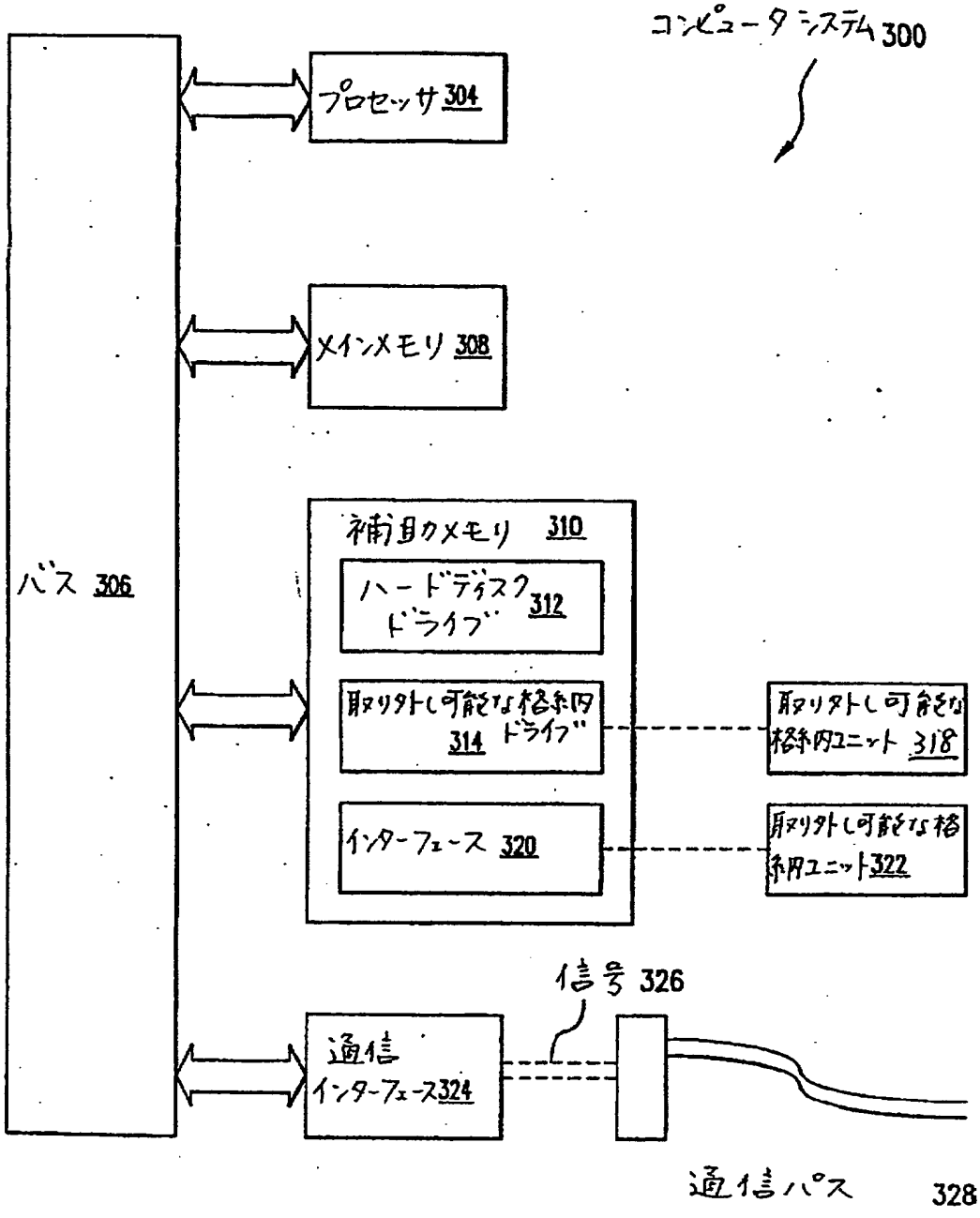
【図１】



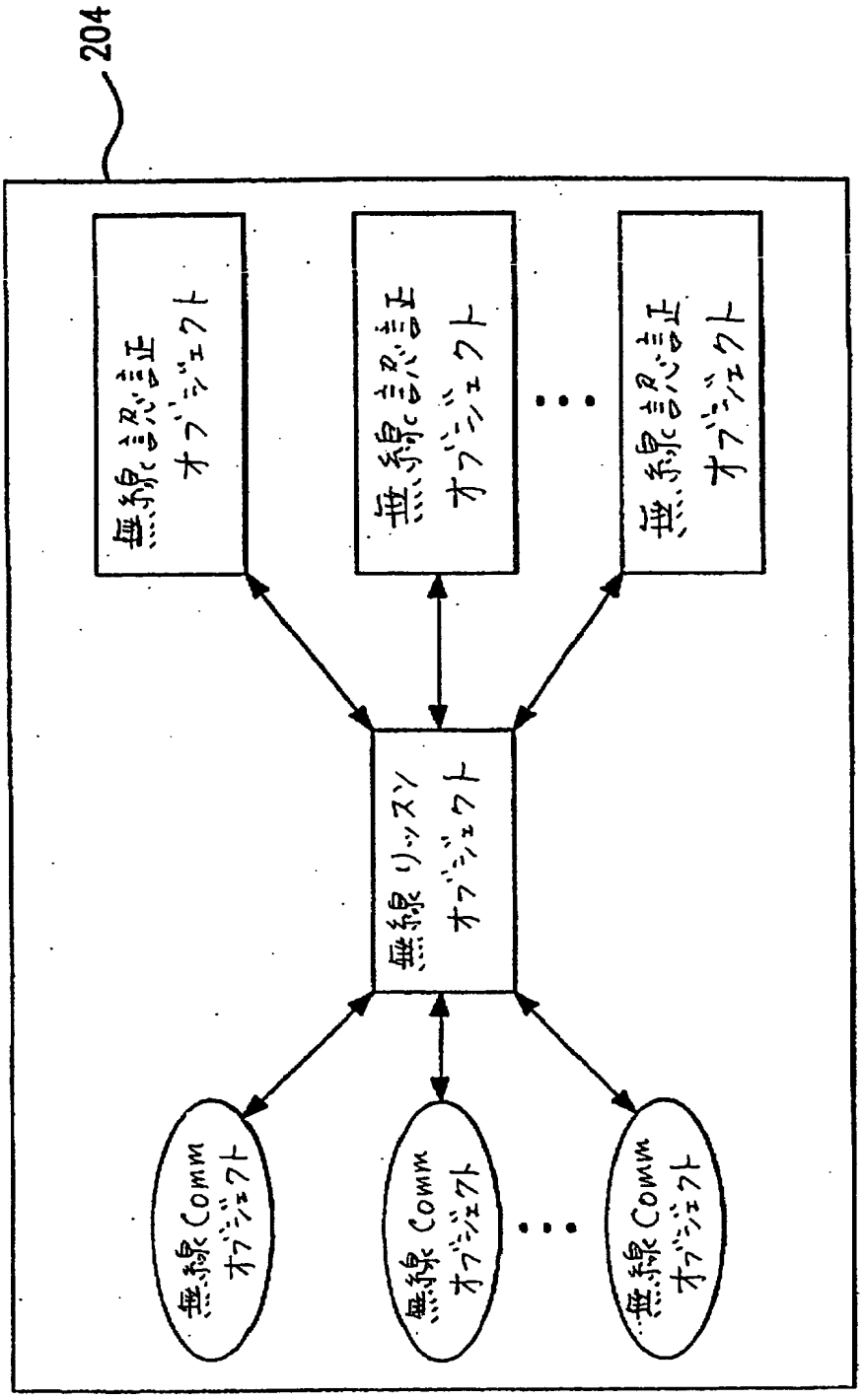
【図２】


202
認証サーバ
204
認証コンポーネント
206
フィルタ
214
ウェブ/アプリケーション
サーバ
208
認証判断
コンポーネント
210
デバイス特有の
コンポーネント
212
ウェブブラウザ
(HTTPI:よってイネーブル
されるクライアント)

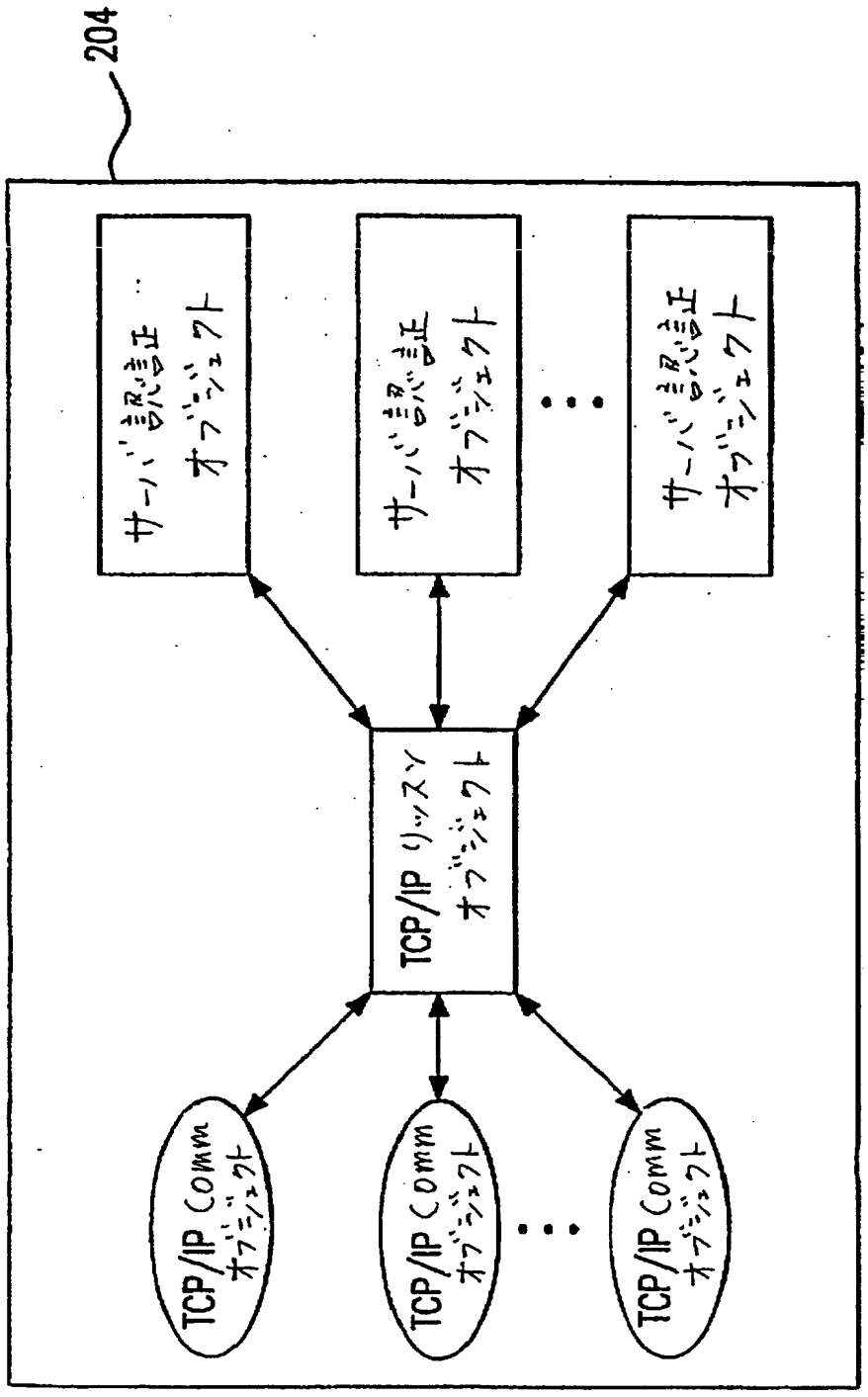
【図３】


コンピュータシステム 300
プロセッサ 304
メインメモリ 308
バス 306
補助メモリ 310
ハードディスクドライブ 312
取り外し可能な格納用ドライブ 314
取り外し可能な格納用ユニット 318
インターフェース 320
取り外し可能な格納用ユニット 322
信号 326
通信インターフェース 324
通信パス 328

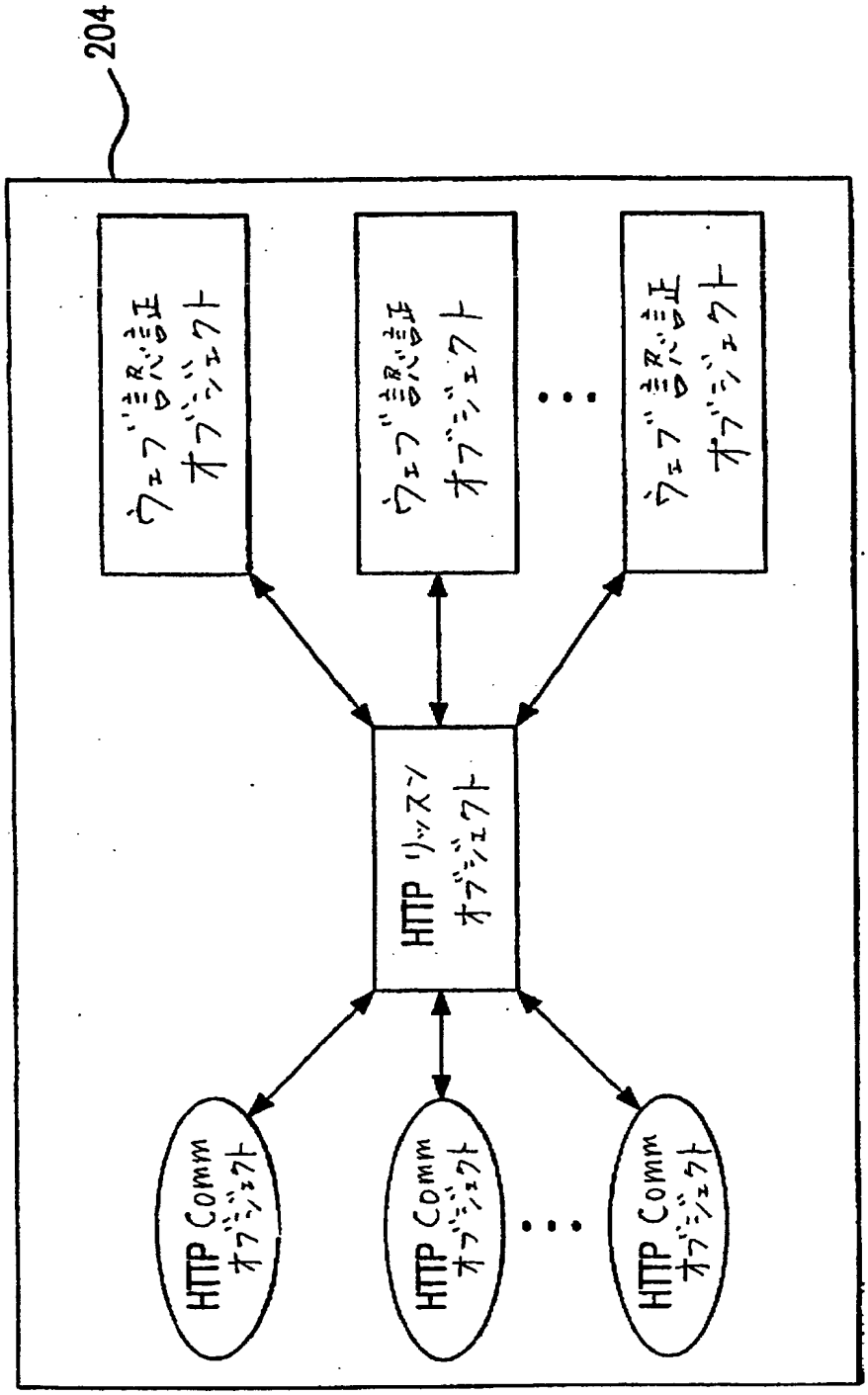
【図４】


204
無線認証
オブジェクト
無線認証
オブジェクト
無線認証
オブジェクト
無線リソース
オブジェクト
無線 Comm
オブジェクト
無線 Comm
オブジェクト
無線 Comm
オブジェクト

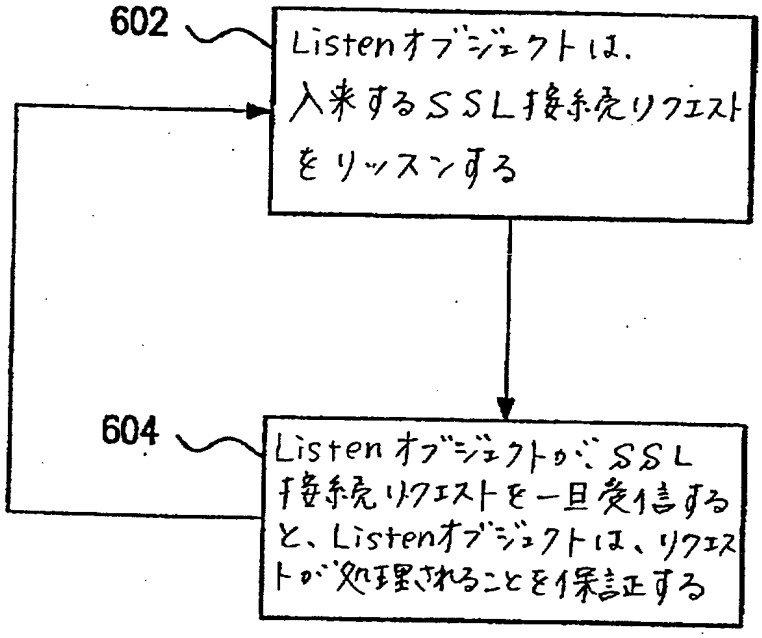
【図５Ａ】


204
サーバ認証オブジェクト
サーバ認証オブジェクト
サーバ認証オブジェクト
TCP/IP リッスン オブジェクト
TCP/IP Comm オブジェクト
TCP/IP Comm オブジェクト
TCP/IP Comm オブジェクト

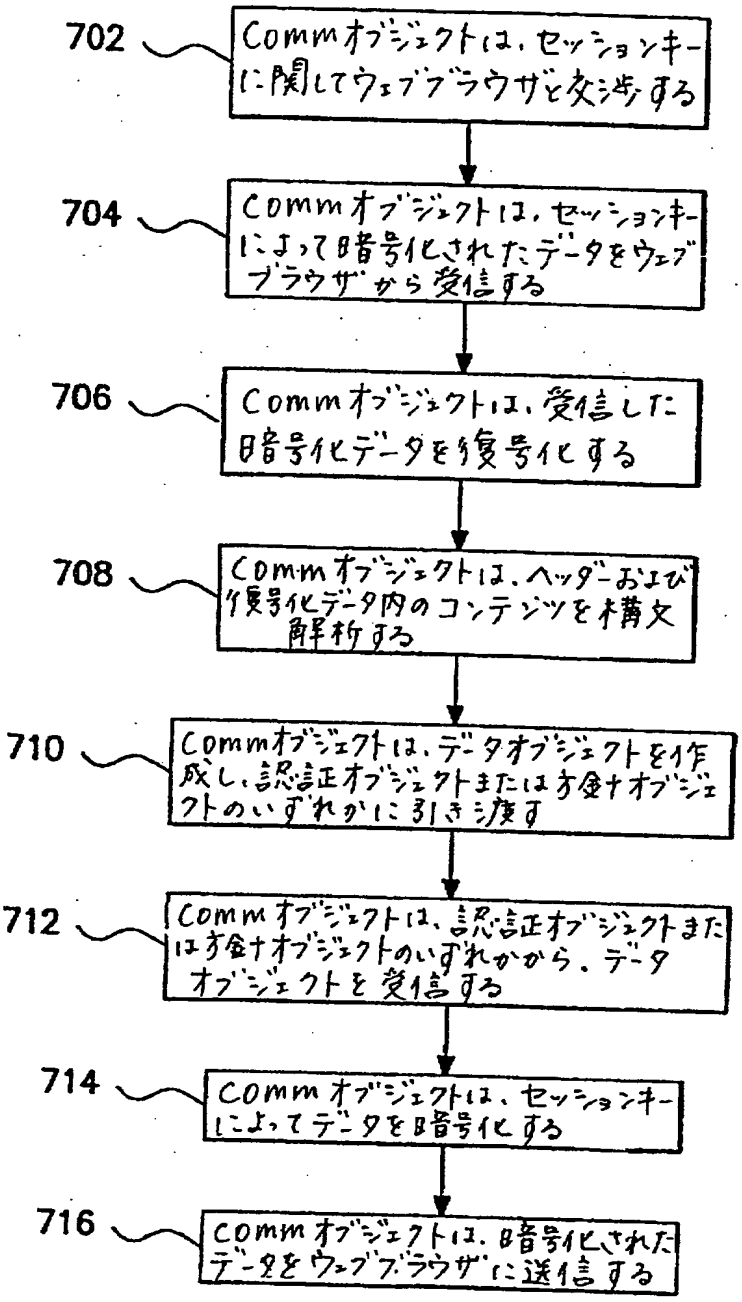
【図５Ｂ】


204
ウェブ認証オブジェクト
ウェブ認証オブジェクト
ウェブ認証オブジェクト
HTTP リソース オブジェクト
HTTP Comm オブジェクト
HTTP Comm オブジェクト
HTTP Comm オブジェクト

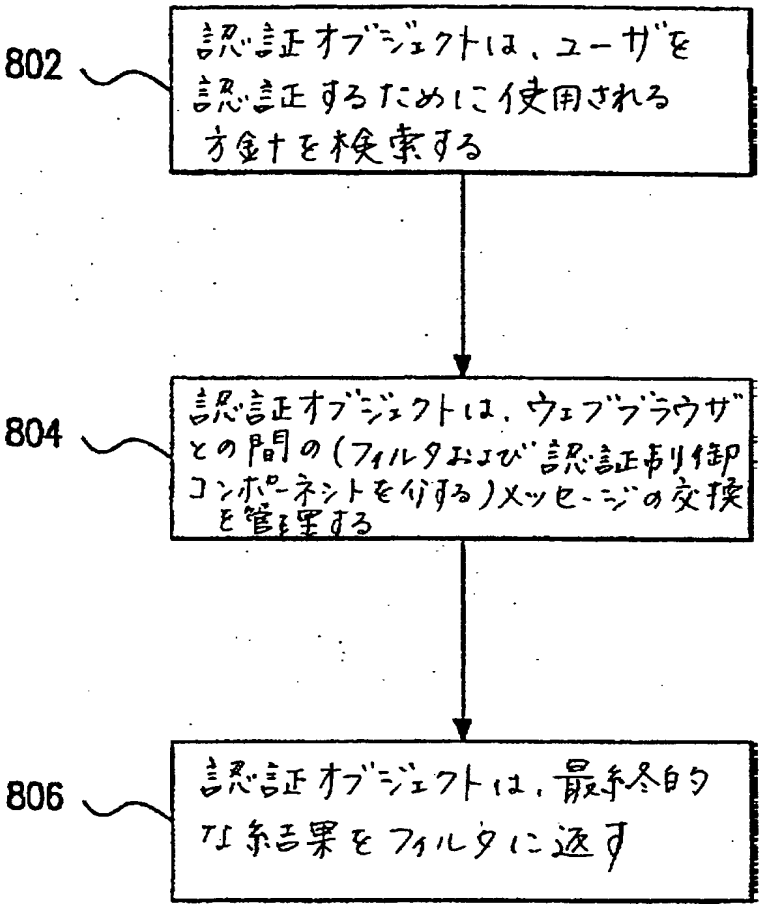
【図６】


602
Listenオブジェクトは、
入来するＳＳＬ接続リクエスト
をリッスンする
604
Listenオブジェクトが、ＳＳＬ
接続リクエストを一旦受信する
と、Listenオブジェクトは、リクエス
トが処理されることを保証する

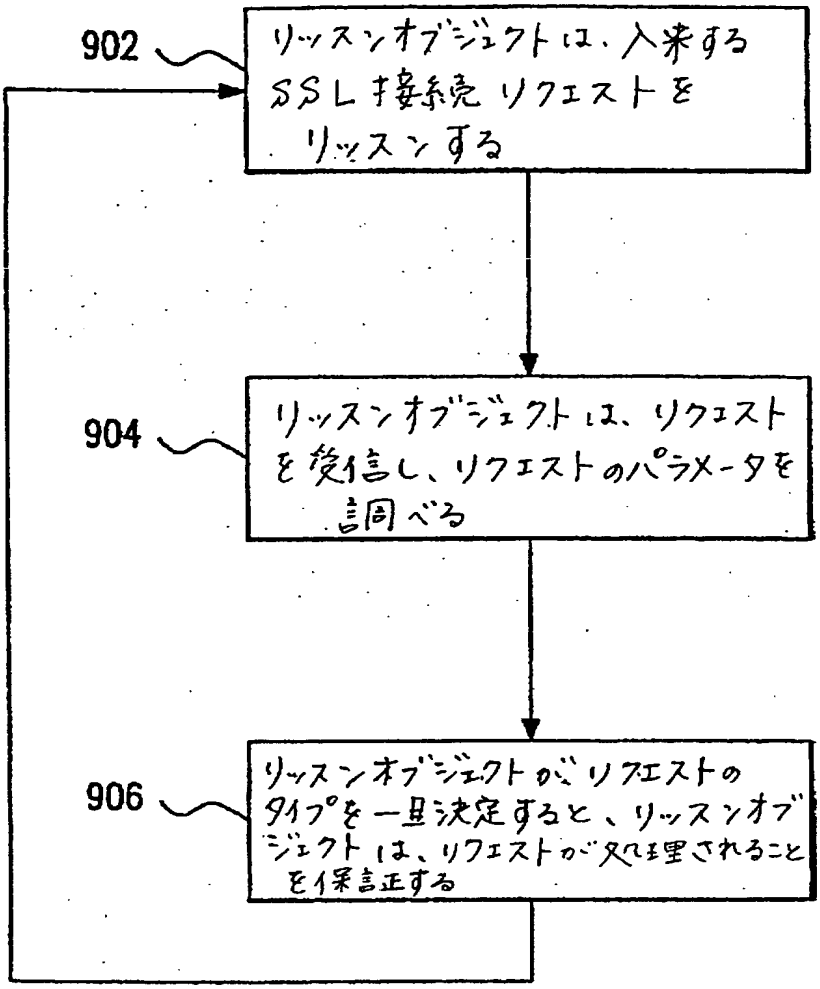
【図７】


702
Commオブジェクトは、セッションキーに関してウェブブラウザと交渉する
704
Commオブジェクトは、セッションキーによって暗号化されたデータをウェブブラウザから受信する
706
Commオブジェクトは、受信した暗号化データを復号化する
708
Commオブジェクトは、ヘッダーおよび復号化データ内のコンテンツを構文解析する
710
Commオブジェクトは、データオブジェクトを作成し、認証オブジェクトまたは予定オブジェクトのいずれかに引き渡す
712
Commオブジェクトは、認証オブジェクトまたは予定オブジェクトのいずれかから、データオブジェクトを受信する
714
Commオブジェクトは、セッションキーによってデータを暗号化する
716
Commオブジェクトは、暗号化されたデータをウェブブラウザに送信する

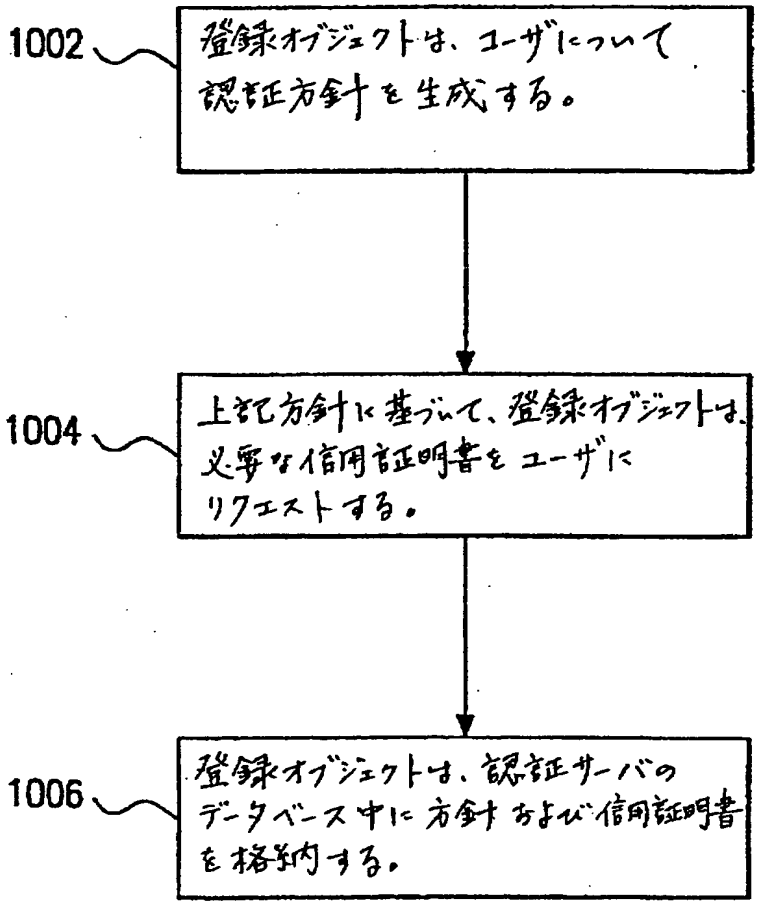
【図８】


802
認証オブジェクトは、ユーザを認証するために使用される方針を検索する
804
認証オブジェクトは、ウェブブラウザとの間の（フィルタおよび認証制御コンポーネントを介する）メッセージの交換を管理する
806
認証オブジェクトは、最終的な結果をフィルタに返す

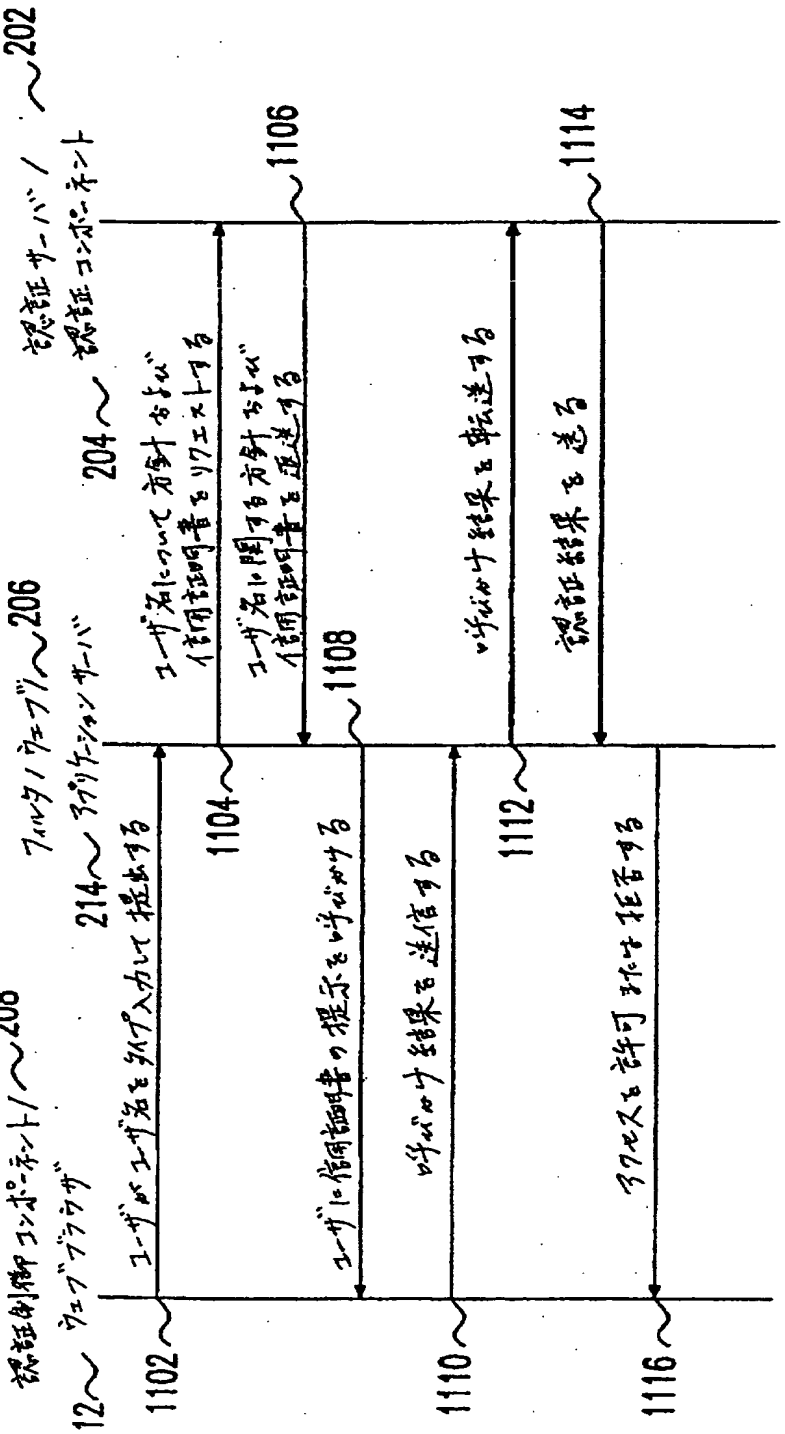
【図９】


902
リッスンオブジェクトは、入来するSSL接続リクエストをリッスンする
904
リッスンオブジェクトは、リクエストを受信し、リクエストのパラメータを調べる
906
リッスンオブジェクトがリクエストのタイプを一旦決定すると、リッスンオブジェクトは、リクエストが処理されることを保証する

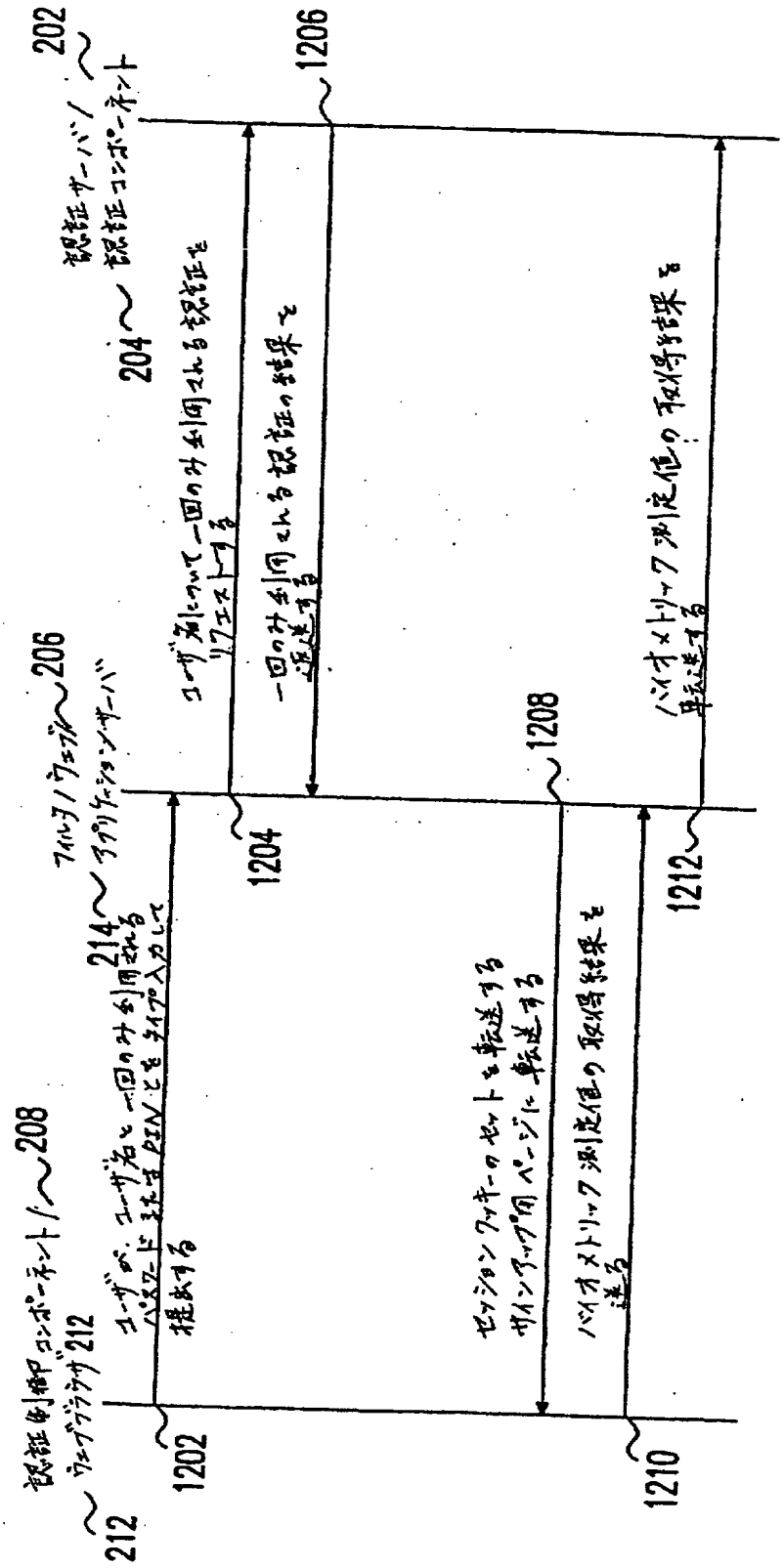
【図１０】


1002
登録オブジェクトは、ユーザについて認証方針を生成する。
1004
上記方針に基づいて、登録オブジェクトは、必要な信用証明書をユーザにリクエストする。
1006
登録オブジェクトは、認証サーバのデータベース中に方針および信用証明書を格納する。

【図１１】


認証制御コンポーネント / 208
ウェブブラウザ 212
ウェブサーバ / アプリケーションサーバ 214
フィルタ / ウェブ 206
認証サーバ / 認証コンポーネント 202
204
1102
1104
1106
1108
1110
1112
1114
1116

【図１２】


認証制御コンポーネント
ウェブブラウザ
212
208
フィルタ/ウェブ
アプリケーションサーバ
214
206
認証サーバ/
認証コンポーネント
204
202
1202
1204
1206
1208
1210
1212
ユーザ名と一回の外利用
パスワードまたはPINとを
タイプ入力して
提出する
ユーザ名について一回の外利用
"リクエスト"する
一回の外利用である認証の結果を
返送する
セッションクッキーのセットを転送する
サインアップ用ページに転送する
バイオメトリック測定値の取得結果を
送る
バイオメトリック測定値の取得結果を
転送する

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US01/03541

A. CLASSIFICATION OF SUBJECT MATTER
IPC(7) :Please See Extra Sheet.
US CL :Please See Extra Sheet.
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED
Minimum documentation searched (classification system followed by classification symbols)
U.S. : 713/200, 201, 202; 705/52, 52, 54; 709/217, 219, 226, 227, 228, 229

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
Please See Extra Sheet.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 6,003,084A (GREEN ET AL) 14 DECEMBER 1999, SEE ENTIRE DOCUMENT	1-24N
X,P	US 6,070,243 A (SEE ET AL) 30 MAY 2000, SEE ENTIRE DOCUMENT	1-24
X,P	US 6,178,505 B1 (SCHNEIDER ET AL) 23 JANUARY 2001, SEE ENTIRE DOCUMENT	1-24
X,P	US 6,182,226 B1 (REID ET AL) 30 JANUARY 2001, SEE ENTIRE DOCUMENT	1-24

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)		
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed	"&"	document member of the same patent family

Date of the actual completion of the international search 20 MARCH 2001	Date of mailing of the international search report 26 APR 2001
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer CHRISTOPHER A REVAK Telephone No. (703) 305-9618

Form PCT/ISA/210 (second sheet) (July 1998)*

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US01/03541

A. CLASSIFICATION OF SUBJECT MATTER:
IPC (7):

G06F 11/30, 12/14, 15/16, 15/173, 17/60; H04L 9/00, 9/32; H04K 1/00

A. CLASSIFICATION OF SUBJECT MATTER:
US CL :

713/200, 201, 202; 705/52, 52, 54; 709/217, 219, 226, 227, 228, 229

B. FIELDS SEARCHED
Electronic data bases consulted (Name of data base and where practicable terms used):

BRS (FILES: USPAT, DERWENT, JPO, EPO, IBM TDB'S)

search terms: policy, filter, filters, filtering, filtered, id, credential, identity, identification, identifying, identified, password, authorize, authority, authorized, authorizing, authenticate, authenticated, authentication, authenticating, request, requesting, requested, access, accessing, accessed, firewall

Form PCT/ISA/210 (extra sheet) (July 1998)*

フロントページの続き

(31)優先権主張番号　６０／１９１，４７１
(32)優先日　平成12年３月23日(2000. 3. 23)
(33)優先権主張国　米国（ＵＳ）
(31)優先権主張番号　０９／６９５，０６０
(32)優先日　平成12年10月25日(2000. 10. 25)
(33)優先権主張国　米国（ＵＳ）
(81)指定国　ＥＰ(ＡＴ，ＢＥ，ＣＨ，ＣＹ，ＤＥ，ＤＫ，ＥＳ，ＦＩ，ＦＲ，ＧＢ，ＧＲ，ＩＥ，ＩＴ，ＬＵ，ＭＣ，ＮＬ，ＰＴ，ＳＥ，ＴＲ)，ＯＡ(ＢＦ，ＢＪ，ＣＦ，ＣＧ，ＣＩ，ＣＭ，ＧＡ，ＧＮ，ＧＷ，ＭＬ，ＭＲ，ＮＥ，ＳＮ，ＴＤ，ＴＧ)，ＡＰ(ＧＨ，ＧＭ，ＫＥ，ＬＳ，ＭＷ，ＭＺ，ＳＤ，ＳＬ，ＳＺ，ＴＺ，ＵＧ，ＺＷ)，ＥＡ(ＡＭ，ＡＺ，ＢＹ，ＫＧ，ＫＺ，ＭＤ，ＲＵ，ＴＪ，ＴＭ)，ＡＥ，ＡＧ，ＡＬ，ＡＭ，ＡＴ，ＡＵ，ＡＺ，ＢＡ，ＢＢ，ＢＧ，ＢＲ，ＢＹ，ＢＺ，ＣＡ，ＣＨ，ＣＮ，ＣＲ，ＣＵ，ＣＺ，ＤＥ，ＤＫ，ＤＭ，ＤＺ，ＥＥ，ＥＳ，ＦＩ，ＧＢ，ＧＤ，ＧＥ，ＧＨ，ＧＭ，ＨＲ，ＨＵ，ＩＤ，ＩＬ，ＩＮ，ＩＳ，ＪＰ，ＫＥ，ＫＧ，ＫＰ，ＫＲ，ＫＺ，ＬＣ，ＬＫ，ＬＲ，ＬＳ，ＬＴ，ＬＵ，ＬＶ，ＭＡ，ＭＤ，ＭＧ，ＭＫ，ＭＮ，ＭＷ，ＭＸ，ＭＺ，ＮＯ，ＮＺ，ＰＬ，ＰＴ，ＲＯ，ＲＵ，ＳＤ，ＳＥ，ＳＧ，ＳＩ，ＳＫ，ＳＬ，ＴＪ，ＴＭ，ＴＲ，ＴＴ，ＴＺ，ＵＡ，ＵＧ，ＵＺ，ＶＮ，ＹＵ，ＺＡ，ＺＷ